Establishing the Particularities of Cybercrime in Nigeria: Theoretical and Qualitative Treatments

By

Suleman Lazarus

PhD by Publication
Volume One

University of Portsmouth
Institute of Criminal Justice Studies
March 2020

This commentary and publications are submitted in part fulfilment of the requirements of the University of Portsmouth for the degree of PhD by Publication

Table of Contents

Evidence for research significance and impact

Volume Two

Abstract

This thesis, which is based on six peer-reviewed publications, is a theoretical and qualitative treatment of the ways in which social and contextual factors serve as a resource for understanding the particularities of 'cybercrime' that emanates from Nigeria. The thesis illuminates how closer attention to Nigerian society aids the understanding of Nigerian cybercriminals (known as *Yahoo Boys*), their actions and what constitutes 'cybercrime' in a Nigerian context. 'Cybercrime' is used in everyday parlance as a simple acronym for all forms of crimes on the internet, whereas 'cybercrime' in a Nigerian context is rooted in socioeconomics and determined by it. In particular, the defrauding of victims for monetary benefit is the most significant theme that emerged from the analysis of Yahoo Boys. While all six publications are situated at the intersections of multiple fields of study, they all share a common endorsement of the constructionist/interpretivist position. The six-published works comprise: [a] three conceptual publications; and [b] three empirical publications. The conceptual publications deconstruct the meanings of multiple taken-for-granted concepts in cybercrime scholarship and develop more robust conceptual lenses, namely: (1) 'Digital Spiritualization'; (2) 'The Tripartite Cybercrime Framework – TCF'; and (3) 'The Synergy between Feminist Criminology and the TCF'. These new conceptual lenses represent the candidate's contribution to developing theory in the field. Alongside this, the empirical section includes three sets of qualitative data, which include: (1) interviews with seventeen Nigerian parents; (2) lyrics from eighteen Nigerian musicians; and (3) interviews with forty Nigerian law enforcement officers. These diverse sources of qualitative data provide a more fully-developed understanding of 'cybercrime' in the Nigerian context (and elsewhere). All six-published works, while individually contributing to knowledge, collectively shed clearer light on the centrality of cultural context in the explanation of 'cybercrime'.

List of Figures

List of Tables

Declaration

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

Suleman Lazarus

Acknowledgements

My profound gratitude goes to my supervisor, Professor Mark Button, for his unconditional support and guidance. I thank members of my family: Jiuwa, O. Lazarus, Elijah, M. Lazarus, Scipio, E. Lazarus, Tanja Lazarus, for their love and patience while I pursue my degrees from 2010 – 2020 (BSc, MSc, and PhD). I am very grateful to Dr Jovan S. Lewis (University of California, Berkeley) for his financial contribution towards my tuition fee. I appreciate excellent references from Dr Sally Mann and Dr Stephen Wyatt in support of my application for this submission. I am also grateful to Mr Geoffrey U. Okolorie, Mr Edward T. Dibiana, Dr Kate Johnston-Ataata and Professor Biko Agozino, for their moral support in challenging times. Last but not least, my gratitude also goes to the following individuals from the London School of Economics and Political Science: [a] Professor Robert Reiner, for informing me on 3rd May 2016 that my work (i.e., the original formulation of the Tripartite Cybercrime Framework), "can be developed into a very good thesis [and] it is probably publishable in a specialist journal now". [b] Professor Tim Newburn, for his comments on systematic steps for collecting lyrical data. [c] Professor Lucinda Platt, for supervising my Master's dissertation and mentoring me after my graduation – her training, stood me in good stead.

The list of publications included (in date order)

• Ibrahim[1], Suleman. (2016a). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice,* 47, 44-57.
• Ibrahim, Suleman. (2016b). Causes of Socioeconomic Cybercrime in Nigeria. In IEEE *International Conference on Cybercrime and Computer Forensic* (ICCCF), Vancouver, BC, Canada (pp. 1-9). *IEEE* Publishing.
• Lazarus, Suleman. (2018). Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists. *Criminology, Criminal Justice, Law & Society*, 19, (2), 63-81.
• Lazarus, Suleman. (2019a). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, 10, (3), 146, 1-20.
• Lazarus, Suleman. (2019b). Just Married: The Synergy between Feminist Criminology and the Tripartite Cybercrime Framework Journal. *International Social Science Journal*, 69, (231), 15-33.
• Lazarus, Suleman, & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, 40, 14-26.

[1] In 2017, I changed my surname from Ibrahim (paternal) to Lazarus (maternal).

Statement on joint authorship

Publication
Lazarus, Suleman & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, 40, 14-26.

[a] I, Suleman Lazarus, conceived and designed the study. [b] My co-author, Geoffrey U. Okolorie, recruited & interviewed the participants. [c] I analyzed and interpreted the data. [d] my co-author verified the interpretation of data. [e] I drafted the whole article. [f] I carried out the critical revisions of the article. [g] My co-author and I read and approved the published version. The "author contribution statements" can also be found on page 25 of the published work.

1. Introduction

'*We write to taste life twice, in the moment and in retrospection*' - Nin (1975, p. 149)

I 'tasted life in the moment' when I was writing, submitting, revising, resubmitting and publishing the series of publications that accompany this critical narrative. Taking the route of a PhD by Publication has offered me the opportunity to look back and reflect critically on the steps of my academic journey which led to this submission for a doctoral degree. In particular, the submission is for a doctorate by retrospective peer-reviewed publications that constitute an independent and original contribution to knowledge. For me, the unconditional offer from the University of Portsmouth to submit my works for a PhD by Publication award is an additional validation of the quality of my independent contributions to knowledge (as set out in the Level 8 Doctoral Descriptor contained in the UK Quality Code for Higher Education, 2014). While this submission includes a set of six publications published in six different outlets (e.g. International Social Science Journal; Telematics and Informatics), these publication venues are interdisciplinary in orientation and international in scope. All these publications (Ibrahim, 2016a; Ibrahim, 2016b; Lazarus, 2018; Lazarus, 2019a; Lazarus, 2019b; Lazarus & Okolorie, 2019), have consequently been rigorously examined by a set of experts from multiple fields of study.

All six-published works are related. Each one of them is a contextual inquiry that seeks to shed a clearer light on the cultural and social dimensions of cybercrime. In exploring local cultures, all publications acknowledge that in a digital and global age, the actions of criminals have international connections and consequences (Button & Tunley, 2014; Hall & Scalia, 2019; Lewis, 2018; Silverstone, 2013). All publications are also in a similar vein in exploring the convergence of multiple fields

of study (e.g. cultural criminology, social psychology, cyber criminology and religious studies) to examine cybercrime, particularly but not solely, in a Nigerian context. Consequently, they have a similar overarching theme and agenda. [a] They illuminate how closer attention to Nigerian society aids an understanding of the Nigerian cybercriminals (Yahoo Boys) and their actions. [b] They shed light on the particularities of cybercrime by highlighting on the category of cybercrime to which Nigeria is most vulnerable – socioeconomic cybercrime (e.g. cyber-fraud). Because these publications radiate from the same overarching theme and agenda, each of them particularly demonstrates that 'the defrauding of victims for monetary benefits is the most significant theme in the analysis of Nigerian cybercriminals' (e.g. Lazarus, 2018, p. 64; Lazarus, 2019a, p. 2). They have many additional commonalities, some of which are outlined in Figure 1.

Figure 1. Some commonalities of the six publications included

Figure 1 exemplifies that while I have compartmentalised these six publications into publishable parts, they represent a coherent whole body of work (a research portfolio). In a nutshell, they are all based on the premise that cybercrimes and cybercriminals are shaped by cultural and contextual forces, and consequently, they have to be understood as social products and social actors respectively (Ibrahim, 2016a; Ibrahim, 2016b; Lazarus, 2018; Lazarus & Okolorie, 2019; Lazarus, 2019a; Lazarus, 2019b). My earlier work[2] excluded here (i.e. Ibrahim, 2015) which analysed the value of cultural and familial forces in understanding juvenile delinquency in Nigeria and Ghana, was the starting point for the six contextual inquiries included in this submission. In particular, Ibrahim (2015) influenced me at the early stage of my academic writing to examine specific social contexts to understand crime.

I have produced the above series of works over a period of five years (2014 to 2019) during which I had different affiliations, namely [a] 'Royal Holloway University of London' as a postgraduate student (Ibrahim, 2016a; Ibrahim, 2016b); [b] 'Independent Researcher' (Lazarus, 2018); and [c] 'University of Greenwich' as a visiting lecturer (Lazarus, 2019a; Lazarus, 2019b; Lazarus & Okolorie, 2019). For me, my life experience during this space of time and the six publications listed above, which mirror these affiliations/transitions, are two sides of the same coin. Thus, the introductory part of this reflective narrative is couched in three parts [1] my life experiences; [2] the consequences of my experiences (i.e. the mastering of scholarly writing and publishing); and [3] the structure of the rest of the critical commentary.

[2] The book chapter was extracted from my Master's dissertation (the London School of Economics & Political Science).

1.1.My Life Experiences

In his analysis of *Man's Search for Himself,* May (1953) noted that life experience is often the architect of a person's decisions as well as the guide to their path. My negative experience with PhD supervisors, depicted in *Betrayals in Academia and a Black Demon from Ephesus* (Lazarus, 2019c), played a primary role in changing the direction of my PhD route (from my initial enrolment at the Royal Holloway University of London). Confident in my ability to develop ideas at a high level of abstraction (e.g. Ibrahim, 2015; Ibrahim, 2016a; Lazarus, 2019a; Lazarus, 2019b) and act independently with originality in applying new research approaches (e.g. Lazarus, 2018; Lazarus & Okolorie, 2019), I embraced the challenges and responsibilities (e.g. money issues) of an independent researcher, without knowing precisely what lies beyond 'the publication point'. Despite this, I have been intrinsically motivated in researching multiple topics of inquiry. They include both the publications I have included in this research portfolio (e.g. Lazarus, 2018; Lazarus, 2019a; Lazarus, 2019b) and those I have excluded (e.g. Lazarus et al., 2017; Lazarus, 2019d; Rush & Lazarus, 2018). I was firmly convinced that making a significant contribution to knowledge is an invaluable 'currency in academia' (Soule, 2007, p. 6; Starrs, 2008, p. 1) and other domains of life. Retrospectively speaking, choosing to change the direction of my initial doctoral journey enabled me to explore a more appealing, fulfilling and independent way of arriving at my destination, that is, obtaining a doctoral award and solidifying my membership of the academic community.

The life events discussed above highlight that the critical step to a new beginning is to conceive that one is possible. I firmly believe that human suffering, e.g. negative life experiences, could be transformed into human achievement depending on the stand the experiencer takes when faced with it (Frankl, 1978). The inherent

satisfaction in flipping my negative experience and turning it into my achievements has been the impetus behind many publication efforts and the methodological innovation developed (e.g. Lazarus, 2019b; Lazarus & Okolorie, 2019). Metaphorically speaking, therefore, the debris of a negative set of my experiences (described in Lazarus, 2019c) and triumph (depicted in Lazarus, 2020), transformed me into an independent scholar whose contribution has an impact on other authors' works (e.g. De Kimpe et al., 2020; Orji, 2019; Park et al., 2019). This would not have been possible had I given up or remained in the previously restricted route of the traditional PhD model (as I had experienced it at the Royal Holloway University of London).

1.2. The Mastering of Scholarly Writing and Publishing

Within the pedagogy of traditional PhD models, the 'issues of writing and publication' are not systematically and adequately addressed in its design and approach (Lee & Kamler, 2008, p. 511). Academic writing/publishing is, as Jalongo, Boyer, & Ebbeck (2014, p. 241) observed, 'a constellation of skills, understandings, and dispositions too important to be left to chance'. Becoming an independent researcher has facilitated mastering the skills required not only in the selection of appropriate outlets for my manuscripts but also in dealing with negative and positive responses from anonymous journal reviewers and editors. But that is not all. Becoming an independent scholar equipped me with the pragmatism needed in navigating what Manson & Merga (2018b, p. 140) have called 'the politics of publishing' or 'the rules of the game' (Wilkinson, 2015, p. 99). The redirection of my PhD route allowed me to engage more actively with many examiners[3] involved in

[3] The role of the examiners (e.g. anonymous reviewers) is as significant as that of my research mentors. For example, I had revised parts of my manuscripts based on my mentors' comments.

different layers of the publication process. These active engagements with experts in the multiple fields of study have benefits. They have, for example, equipped me with skill sets, 'understanding and dispositions too important to be left to chance' (Jalongo, Boyer, & Ebbeck, 2014). For me, mastering the negotiations, dialogues and pragmatism with these gatekeepers of the publication venues was an invaluable apprenticeship in its own right. It enabled me to adapt my writing to a wide variety of audiences and disciplines such as religious studies (Lazarus, 2019a), feminist criminology (Lazarus, 2019b) and social psychology (Lazarus, 2018).

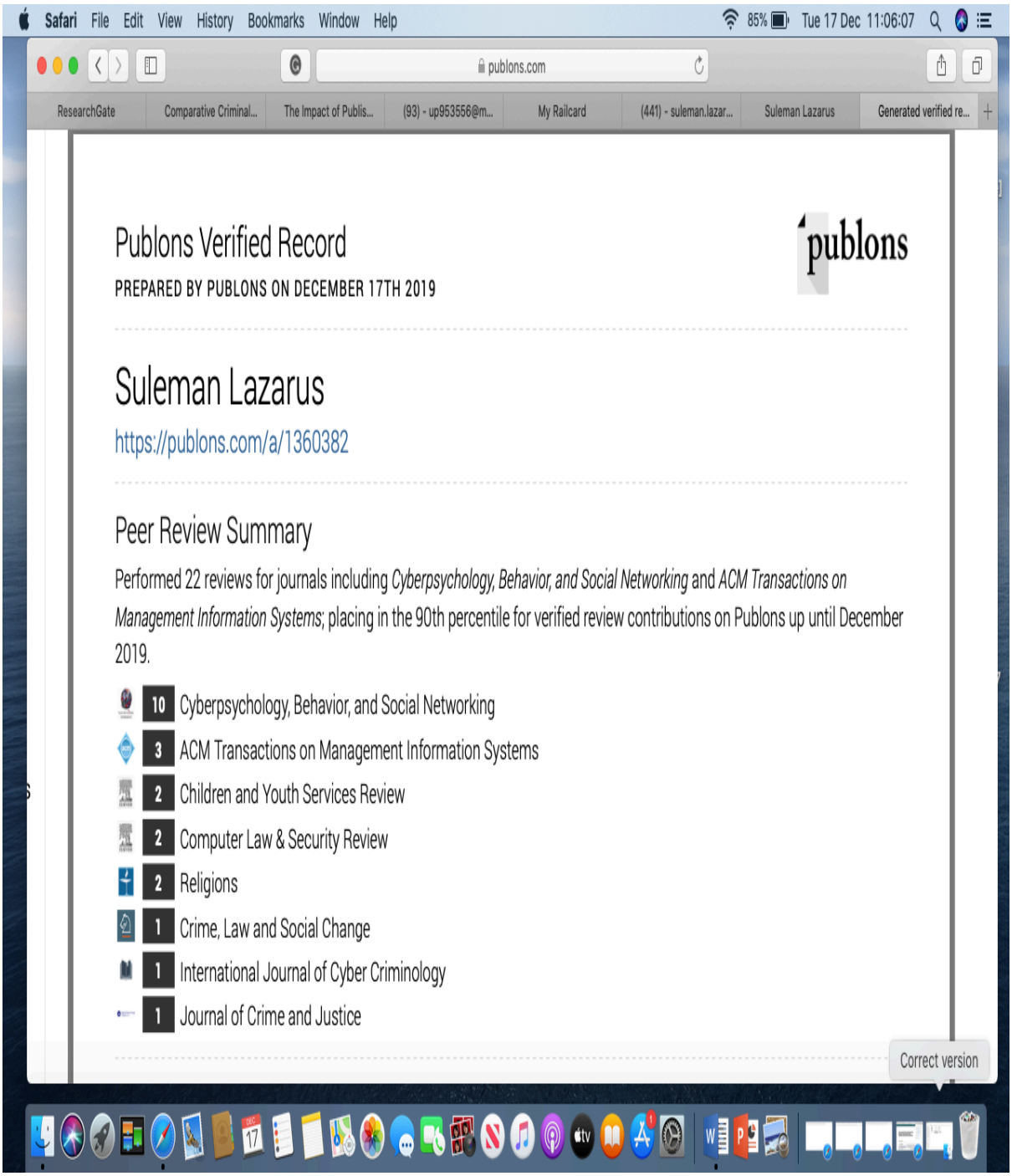
Notably, this type of apprenticeship in becoming an independent scholar is not a core aspect of conventional PhD training (Manson & Merga, 2018a; Manson & Merga, 2018b; Peacock, 2017). Consequently, as Peacock (2017, p. 130) observed, 'All too often, doctoral candidates who have followed the traditional PhD route fail to publish after completing their studies' (see also Francis et al., 2009). Therefore, it is not far-fetched to attribute my mastering of scholarly writing and publishing, to a great extent, to the redirection of my PhD from a traditional one to a PhD by Publication. Becoming an independent author of many peer-reviewed publications has also opened a window of opportunity for me to be in constant dialogue with fellow authors as a reviewer.

In particular, from 2017 to 2019, I have reviewed papers authored by other scholars twenty-two times. I have served as a referee for eight reputable journals as verified by *Publons*[4] (shown in Figure 2). In retrospect, this role has enhanced the confidence and maturity demonstrated especially in my most recent conceptual outputs (e.g.

[4] Publons is a website that provides a free service for academics to track, verify, and showcase their peer reviews and editorial contributions for academic journals.

Lazarus, 2019a; Lazarus, 2019b) as well as the empirical ones (e.g. Lazarus & Okolorie, 2019) as having the opportunity to read multiple revised versions of other authors' works prior to publication has informed my understanding of the writing process.

Figure 2: Dialogues with Fellow Authors and Verified Reviews

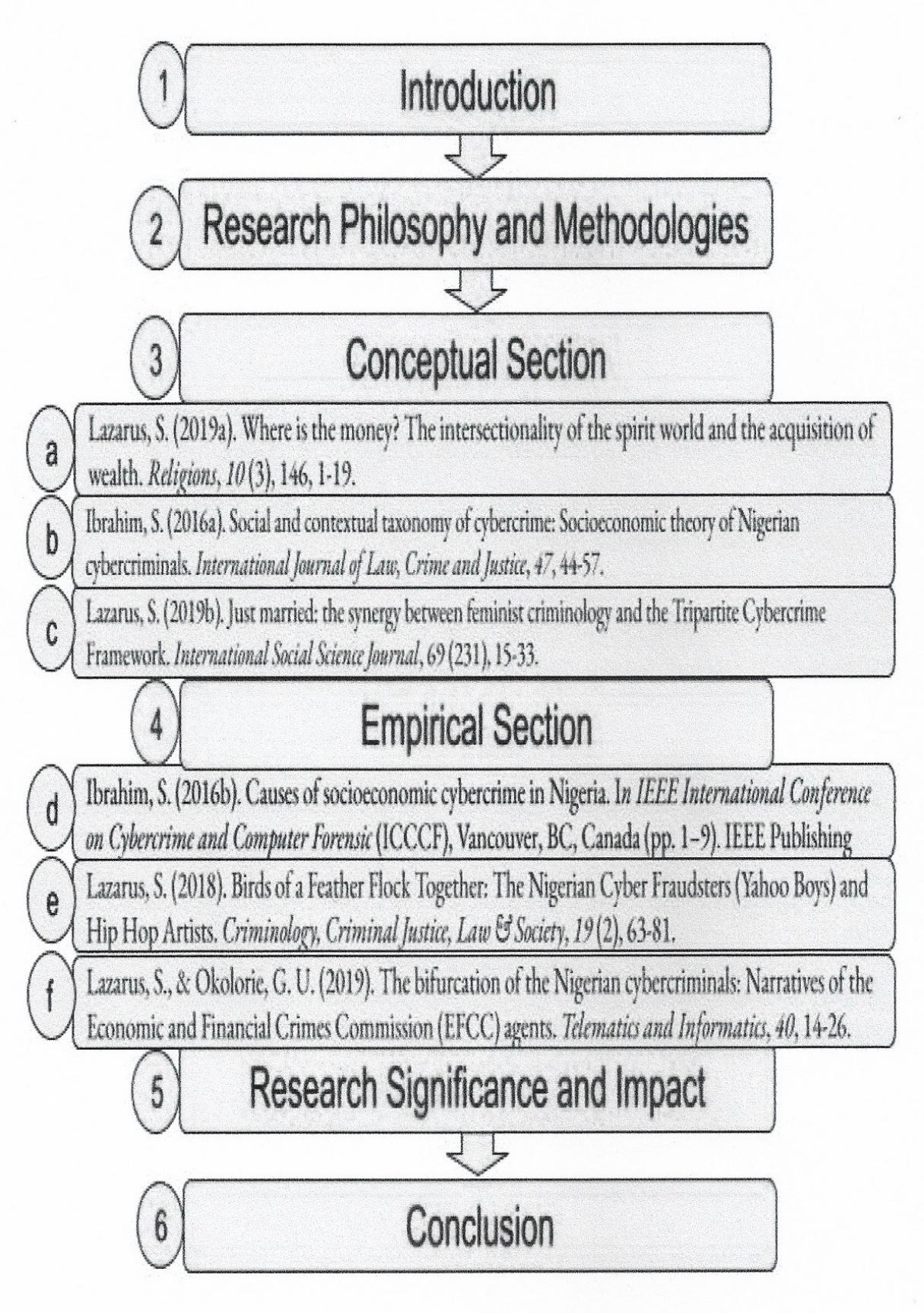


1.3. The structure of the critical commentary

After the introduction (i.e. section 1.1; 1.2), it is now necessary to comment on the rationale for the structure of the rest of the critical commentary. While I listed the six publication outputs sequentially in publication date order above (see *'List of publications included'*) as recommended by the University of Portsmouth (2019), publication dates in themselves do not always represent the writing and submission timeline. Manuscript submission and publication dates do not always progress serially. For example, Lazarus (2019a) was subjected to high inter-reviewer disagreements, and multiple rounds of reviews and resubmissions from 2015 to 2019, whereas, Lazarus (2019b) was submitted in 2018 and published in 2019. The rest of this accompanying narrative, therefore, acknowledges that publication dates are not necessarily a true reflection of the actual dates I drafted and submitted manuscripts to publication venues.

Consequently, the storyline of this reflective narrative favours the pattern of my intellectual thinking and writing rather than publication dates. The rationale is to create a cohesive whole since blueprints about 'structural possibilities for a PhD by Publication are very much emergent' (Manson & Merga, 2018a, p. 1453). For instance, some candidates who graduated from the University of Portsmouth (e.g. Pycroft, 2014) and other UK universities (e.g. Hearsum, 2015) have relied on the particularities of their publication outputs to tell the stories of the accompanying narratives. Based on the preceding remarks, I organise the critical narrative as illustrated in Figure 3.

Figure 3: - Overview of the structure of the accompanying narrative



As illustrated in Figure 3, the remaining aspects of the critical commentary are presented chronologically in five main parts (i.e. [1] section 2 to 6; [2] research philosophy and methodologies; [3] conceptual part; [4] empirical part; [5] research significance and impact; and [6] conclusion. The overview of research philosophy and methodologies (i.e. section 2) deals with the ways in which different layers of the research are connected as a whole. The conceptual part (i.e. section 3) includes three publications (i.e. Lazarus, 2019a; Ibrahim, 2016a; Lazarus, 2019b), and is comprised of two subsections (subsection 3.1. rationale for inclusion; 3.2. contribution to knowledge). These conceptual publications are couched in such a way as to address two core requirements for this accompanying commentary (i.e. rationale for inclusion; contribution to knowledge) as recommended by the University of Portsmouth (2019).

The empirical part (section 4), also comprises of two sub-sections (4.1; 4.2). Like the conceptual section, it also covers three published works. These three empirical outputs (i.e. Ibrahim, 2016b; Lazarus, 2018; Lazarus & Okolorie, 2019) are also examined in terms of 'rationale for inclusion' (4.1); and 'contribution to knowledge' (4.2). While the conceptual lenses facilitate the empirical studies by providing relevant background, the empirical ones substantiate the conceptual ones. In section 5, I discuss research significance and the impact of the whole research portfolio. Like 'rationale for inclusion' and 'contribution to knowledge', 'research significance/impact' is also a core requirement of this accompanying commentary as recommended by the University of Portsmouth (2019). I conclude in section 6.

2. Research philosophy and methodologies

The philosophical background of research is at the base of the researcher's thought in creating new knowledge in the field of study (Fazlıoğulları, 2012; Žukauskas, Vveinhardt & Andriukaitienė, 2018). It is the basis of the research paradigm, consisting of three interconnected components: ontology, epistemology and methodology (as outlined in Table 1 adopted from Žukauskas, Vveinhardt & Andriukaitienė, 2018, p. 121). Consequently, like some 'cybercrime' researchers (e.g. Button & Tunley, 2014; Sugiura, 2018; Wall, 2012; Yar & Steinmetz, 2019), I have approached cybercriminals and their actions from the standpoint of society. In particular, the sets of publications I have included here are situated at the intersection of two related philosophical positions: constructionist and interpretivist perspectives. While the constructionism position refers to the social construction of reality more broadly (e.g. Becker, 1967; Cohen, 1972), the interpretivist position emphasises inter-subjectively in seeking the meaning in actions (e.g. Thomas, 1923; Thomas & Thomas, 1928). The constructionist perspective generally operates more on a macro level and is concerned with how the world is socially constructed (Berger & Luckmann, 1966); whereas the interpretivist standpoint generally operates on a micro level and is concerned with how social actors and their actions are interpreted (Thomas, 1923). In other words, constructivism is more about inter-group relations than interpretivism, which is more about individual social psychology.

Central to constructionist and interpretivist perspectives, however, is the overlap in their accounts of the social origins of knowledge (Tannenbaum, 1938; Thomas, 1923). Additionally, for both positions, one cannot locate a transcendent truth, a 'truly true' and there is no one truth for all cultures at all times (Gergen & Gergen, 2012, p. 3). Indeed, both seemingly different positions are intertwined in the sense that in

seeking a greater understanding of social life, the interpretation of actions and actors is ultimately socially and situationally constructed (Thomas, 1923; Schwandt, 1998).

Table 1. Three components of a research paradigm

Components	*Description*
Epistemology	General philosophical parameters and assumptions that deal with the creation of knowledge (how we know what we know).
Ontology	General philosophical parameters and assumptions that deal with the fundamental nature of reality (and asks what reality is).
Methodology	Combination of different techniques used by researchers to explore different situations.

Adopted from Žukauskas, Vveinhardt & Andriukaitienė (2018, p. 121)

The constructionist/interpretivist position upon which the six publications (Ibrahim, 2016a; Ibrahim, 2016b; Lazarus, 2018; Lazarus, 2019a; Lazarus, 2019b; Lazarus & Okolorie, 2019) sit, has been adopted, for example, by the first Chicago sociologists (e.g. Tannenbaum, 1938; Thomas, 1923) and the later Chicago scholars (e.g. Becker, 1967; Matza & Sykes, 1961). These sociologists (e.g. Tannenbaum, 1938; Matza & Sykes, 1961) have argued that criminality emerges out of offenders' social environments, interactions with others, and life experiences.

Within this broad constructionist/interpretivist philosophical position, I employed several theoretical orientations (e.g. feminist perspective, Lazarus, 2019b; moral disengagement mechanisms, Lazarus, 2018). These all share a similar notion that the interpretation of actions and actors is socially and situationally constructed. I have done so to benefit from a dialogue between the different theoretical perspectives. This dialectical approach enabled me (e.g. Lazarus, 2019a; Lazarus, 2019b) to merge

divergent abstractions to expand and deepen, rather than simply confirm the existing understanding in the field. I have, for example, deconstructed the singular meaning of cyber spiritualism in the existing literature and proposed a binary one (Lazarus, 2019a). Other authors have validated my claim (e.g. Orji, 2019). The constructionist/interpretivist philosophical position, which highlights the significance of subjective experience in human social life, has shaped my research questions. These research questions and their key achievements are listed in Table 2.

Table 2. Research questions and achievements

Published Works	Research Question(s)	A Key Achievement
Lazarus (2019a)	➢ In what ways are the actions of youths who tap spiritual resources for online gain a reflection of local epistemologies and worldviews in Nigeria? ➢ Are these actions alien in the body of Nigerian society?	➢ The article deconstructed the singular meaning of cyber-spiritualism through its development of 'digital spiritualization' and proposed a dual meaning (licit and illicit).
Ibrahim (2016a)	➢ How useful are the existing cybercrime taxonomies in making sense of social and contextual factors? ➢ Since 'cybercrime' is a globalised phenomenon, how is the Nigerian case any different from Western regions? ➢ What exactly is 'cybercrime' in a Nigerian context?	➢ The article critiqued the prevailing taxonomies used in cybercrime scholarship through its development of the Tripartite Cybercrime Framework (TCF) which proposed that cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical.

Lazarus (2019b)	➢ Do structured gender relations retain their efficacy in online contexts? ➢ Do gender forces in society influence online behaviours and experiences?	➢ The article built synergy between the feminist epistemology of crime and the Tripartite Cybercrime Framework to advocate the centrality of gender as a theoretical entry point for the investigating of all aspects of cyber criminology.
Ibrahim (2016b)	➢ What are parents' perceptions of the causes of cybercrime involvement among Nigerian children?	➢ The perceptions of Nigerian parents (n=17) underscored that a range of familial factors such as 'a good family environment' has more influence on a person's susceptibility to involvement in cybercrime than external factors such as corruption.
Lazarus (2018)	➢ What are the ethics of Nigerian cyber-criminals as expressed by music artists? *The ethics of Yahoo Boys can be understood as a set of perceptual alterations that offer them 'psychological shields' to justify their conduct and thus, circumvent self-condemnation (drawing from Bandura, 1999; Sykes & Matza, 1957).* ➢ Which techniques do artists deploy to	➢ The lyrics of hip-hop artists (n=18) exposed the presence of the mechanisms of moral disengagement (Bandura, 1999) and neutralization techniques (Sykes & Matza, 1957) in cyber-fraud victimisation.

	describe cyber-criminals and their victims? ➢ What might the justifications say about the motives for 'cybercrime'?	
Lazarus & Okolorie (2019)	➢ What are the narratives of frontline law enforcement officers about cyber-fraudsters and their activities in Nigeria?	➢ The narratives of law enforcement officers (n=40) distinguished the Nigerian cybercriminals and their operations based on three factors: educational-attainment, modus-operandi, and networks-collaborators.

In answering the research questions listed above, all six publications are situated at the intersection of multiple fields of study. While some of them are listed in Table 3, all these fields share a common endorsement of the constructionist/interpretivist position.

Table 3. Intersections of multiple fields of study

Fields of study	**Publications**
➢ Cyber criminology ➢ Cultural criminology ➢ Cultural sociology ➢ Social psychology	All six publications in this submission
➢ Religious studies	e.g. Lazarus (2019a)
➢ Feminist criminology	e.g. Lazarus (2019b)
➢ Musicology	e.g. Lazarus (2018)
➢ Youth studies	e.g. Ibrahim (2016b)

In particular, the constructionist/interpretivist lens has enabled me in my conceptual publications to [a] deconstruct the meanings of some taken-for-granted concepts in cybercrime scholarship and [b] develop more robust conceptual lenses, namely (1) 'Digital Spiritualization' (Lazarus, 2019a); (2) 'The Tripartite Cybercrime Framework – TCF' (Ibrahim, 2016a); and (3) 'the synergy between Feminist Criminology and the TCF' (Lazarus, 2019b). My development of the above new conceptual lenses is invaluable in the field, and this achievement is worth much more when one considers that theoretical originality is the arena where marginalised voices on the Nigerian cybercriminals are most vulnerable. Equally, the development of these new conceptual lenses in themselves serves as a part of my 'contribution to developing theory in the field' as outlined by the University of Portsmouth (2019, p. 1) concerning a PhD by Publication award.

Similarly, the constructionist/interpretivist lens is significant for the empirical studies. Thus, the constructionist/interpretivist lens has also shaped the methods deployed in the three qualitative studies. These studies (Ibrahim, 2016b; Lazarus, 2018; Lazarus & Okolorie, 2019), in particular, acknowledge that 'a man is like an insect suspended and enveloped in spider webs of culture, and the analysis of it and its actions must go in search of meaning and subjective experience' (Geertz, 1973, p. 3). This is because, 'the focus was on meanings and understandings rather than representative populations and generalising the data' (Sugiura, 2016, p. 147). People's words provide greater access to their experience of the world and what they construct as a reality in their stories than statistical trends (Lazar, 2008). Consequently, I have favoured qualitative approaches to illuminate how closer attention to Nigerian society aids the understanding of Yahoo Boys and their actions.

These studies (Ibrahim, 2016b; Lazarus, 2018; Lazarus & Okolorie, 2019) include three sets of data collected from three different sources and times. First, Ibrahim's (2016b) study is based on interviews with 17 Nigerian parents. Second, Lazarus's (2018) study involves a qualitative analysis of lyrical data from 18 Nigerian hip-hop artists. Third, Lazarus & Okolorie's (2019) study is based on interview data derived from 40 Nigerian law enforcement officers. Lazarus's (2018) study relied solely on online data in the public domain (lyrics), and ethical approval for this type of research as Sugiura, Wiles & Pope (2017, p. 195) observed, is 'neither possible nor necessary'. Conversely, the two interview studies (Ibrahim, 2016b; Lazarus & Okolorie, 2019) required ethical approvals, and I obtained ethical approval from the Royal Holloway University of London for Ibrahim's (2016b) study. Similarly, my co-author (i.e. Lazarus & Okolorie, 2019) who recruited and interviewed participants 'on the ground', obtained ethical approval for the study in Nigeria. These three qualitative studies are distinctive in the ways outlined in Table 4 below.

Table 4. The distinctiveness of the three qualitative studies

Qualitative Study	*Empirical Basis*	*A Key Distinctiveness*
Ibrahim (2016b)	Interview data: n=17 parents	The first peer-reviewed empirical study to explore the intersectionality of family factors and cyber criminality in a Nigerian context.
Lazarus (2018)	Lyric data: n=18 musicians	The first peer-reviewed empirical study to examine the ways the Nigerian cybercriminals are represented in hip-hop music.
Lazarus & Okolorie (2019)	Interview data: n=40 law enforcement officers	The first peer-reviewed empirical study to explore the narratives of the Economic and Financial Crimes Commission officers concerning the Nigerian cybercriminals.

For me, these seemingly different sources of qualitative data (parents, music artists, and law enforcement officers) come together to paint a clearer image of the central theme of my inquiry – cultural and social dimensions of cybercrime in a Nigerian context. Data from these three groups of Nigerians, while making individual contributions to knowledge (outlined further down), collectively shed a clearer light on the topic from their unique lenses. It is noteworthy that this critical narrative does not contain an additional section designated as the 'methodologies' or 'literature review', as the relevant methodology and literature review are within each publication output and by implication, a separate section would be redundant and repetitive (Manson & Merga, 2018a).

In retrospect, however, I would have done some things differently. Every achievement is subject to improvements as Freud (1927) observed. For example, Lazarus (2018), in its analysis of 'maga' would have benefited from Mills's (1940) original formulation of the concept of the vocabulary of motive. Equally, Ibrahim (2016b), would have benefited from using the lens of decolonisation to look more critically at the concept of 'juvenile delinquency[5]'. Having outlined the ways in which the six-published works are connected to a broad philosophical position, it is necessary to focus on the rationales for including them in this research portfolio.

3. Conceptual publications

3.1.Rationale for inclusion

The three conceptual articles ([1] Lazarus, 2019a, [2] Ibrahim, 2016a, and [3] Lazarus, 2019b) included are couched at different levels of abstraction as detailed below. I

[5] Historically, the British Government introduced the concept of 'juvenile delinquency' to the Federal Republic of Nigeria through colonialism (Ibrahim, 2015).

have included these publications because they not only critique the meaning of the existing concepts, theories and taxonomies in cybercrime scholarship, but they also deconstruct them. However, that is not all. These publications consequently develop new conceptual lenses. These three publications are also related in their deployment of social and contextual factors to challenge the prevailing conceptualisations about cybercrime.

Publication
Lazarus, Suleman. (2019a). Where is the money? The intersectionality of the spirit world and the acquisition of wealth. *Religions*, *10* (3), 146, 1-20.

In this article, I analysed 'the contemporary manifestation of spirituality in cyberspace,' with history in mind, to illuminate the past that created it (Lazarus, 2019a p. 1-16). By doing so, the article developed a useful conceptual lens: 'digital spiritualization,' to deploy a critical examination of the intersectionality of cyber-fraud and spirituality in a Nigerian context. The basis of its inclusion is hinged on five aspects. First, the intersectionality of cyber-fraud and spirituality is a central theme in the discussion of crime in a Nigerian context (e.g. Ellis, 2016). Hence, it would be an oversight to exclude a publication which analysed the spiritual dimension of cyber-fraud in a research portfolio whose overarching agenda is to shed light on the cultural, spiritual and social dimensions of 'cybercrime'. Second, the article serves as a major entry point in establishing the particularities of cybercrime in a Nigerian context. It matters because, while the spiritual dimension of cybercrime is not an aspect of cybercrime in discussions about the Global North (Cross, 2018), Africa south of the Sahara - including Nigeria, is culturally different from the West (Ibrahim, 2015; Ibrahim & Komulainen, 2016; Rush & Lazarus, 2018). Third, the article fits squarely into the overarching theme and agenda. The publication, for example, *devil advocates*[6] the 'righteousness' of law-abiding

[6] Here, the phrase *devil advocating*, means arguing against the 'righteousness' or 'sainthood' of a group (claimed law-abiding citizens) in order to uncover any misrepresentation of the evidence

Nigerians, by highlighting that the line dividing them and cybercriminals is blurred with regards to the use of magical means for material ends (Lazarus, 2019a, p. 1). For me in particular, 'the explanation of cyber-fraud becomes clearer by exploring the Nigerian cybercriminals' similarities to the society that produced them rather than their dissimilarities' (drawing from Matza & Sykes, 1961, p. 719). Fourthly, the original manuscript of this publication which was drafted in 2015 opened an additional portal to unlock other research opportunities (Ibrahim, 2016a; Lazarus, 2019b), such as the need to challenge the classifications of cybercrime in the existing cybercrime scholarship addressed by Ibrahim (2016a).

Additionally, the rationale for including this publication extends to an ongoing research project. To further nuance the intersectionality of the spirit world and the acquisition of wealth, I am currently examining how this intersection is depicted in Nollywood movies. I am also investigating Nigerians' perceptions of theurgy rituals and wealth creation beyond fictional realms to shed a brighter light on the specifics of how spiritualism is incorporated into cybercrime. While I will be analysing these sets of data shortly after the oral defence of this award for a PhD by Publication, I believe the study will help illuminate 'digital spiritualization' far beyond the conceptual realm achieved by Lazarus (2019a).

Publication
Ibrahim, Suleman. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44-57.

This article is included because it developed an invaluable conceptual lens to facilitate the examination of cybercrime in a Nigerian context (and elsewhere).

favouring them (e.g. concerning the use of magical/spiritual powers for wealth generation) (Lazarus, 2019a).

Specifically, it developed 'the Tripartite Cybercrime Framework' (TCF) by incorporating social and contextual factors into the classification schemas. The TCF illustrates that cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical. Thus, I have included this publication because, while the TCF enables me to focus on the category of cybercrime to which Nigeria is most vulnerable – socioeconomic cybercrime – the TCF suggests problems with prevailing taxonomies of cybercrime. Indeed, 'the conceptual pipeline in the Global North cannot hold water in a Nigerian context' (Ibrahim, 2016a, p. 55) because 'life in the virtual world embodies cultural nuances in society' (Lazarus & Okolorie, 2019, p. 15; see also Jaishankar, 2007; McGerty, 2000). Additionally, the TCF provided me with the 'ammunition' to challenge the dominant statistics relied upon to measure the prevalence of cybercrime perpetrators across nations from 2006 to 2010, which aligns with the overarching theme and agenda of this research portfolio. Last, but not least, Ibrahim (2016a) is a foundational article because it distinguishes between hitherto ignored components of cybercrime in its development of the TCF (see Goyanes, 2020, p. 204 on 'foundational articles'). The TCF provided a critical pillar on which another conceptual publication is based (i.e. Lazarus, 2019b).

Publication
Lazarus, Suleman. (2019b). Just married: The synergy between feminist criminology and the Tripartite Cybercrime Framework. *International Social Science Journal*, 69 (231) 15-33.

I have included this publication because it exploits multiple theoretical axes relevant to this research portfolio. First, it builds 'the synergy between feminist criminology and the Tripartite Cybercrime Framework', which brings the lens of intersectionality explicitly into the discussion of this topic of inquiry. While the Nigerian social and contextual factors, for example, serve as a resource for understanding gender and crime connections, it offers additional layers of explanation and facilitates the framing of qualitative publications included in this research portfolio (e.g. Lazarus & Okolorie, 2019). Second, the publication also sharpens the contrast between the

socioeconomic and psychosocial cybercrime types, by considering motivation, victimization, gender experience, gender roles, and social and relationship performance. This contrast is invaluable to the discussion of the centrality of socioeconomic cybercrime in a Nigerian context. Third, the publication also offers a criticism of the General Theory of Crime (GTC) in its discussion of 'self-control' and 'the moral-standard'. This achievement has a direct connection with Ibrahim's (2016b) qualitative study (also included here), which explores the importance of 'self-control' and 'the moral-standard' in the discussion of the Nigerian cybercriminals. Related to this is that while the equilibrium between theory and illustration is challenging for many authors, I did not lose focus on the practical dimension of this article. I have illustrated my conceptual ideas with arrays of case studies not only to achieve a balance between theoretical guidance and examples but also to nuance the intersectionality of cultural, familial, legal factors and cybercrime. Thus, this publication fits squarely with the theme and agenda of this research portfolio.

3.2.Contributions to knowledge

While these conceptual peer-reviewed outputs are inextricably connected, they make arrays of significant contributions to knowledge, which are most revealing in a tabular form. It is best for a doctoral thesis to 'clearly outline or tabulate the different ways in which the work is original' (Gill & Dolan 2015, p. 11). Accordingly, I have outlined key original contributions of the conceptual publications in Table 5, and that of the empirical publications in Table 6.

Table 5. List of original contributions to knowledge (conceptual outputs)

Conceptual publications	*Key contributions to knowledge in the field*
Lazarus (2019a)	➢ The first publication to deconstruct the prevailing meaning of cyber-spiritualism. ➢ The first publication to propose a dual meaning of cyber spiritualism or 'digital spiritualization'. ➢ The publication uses the phrase 'devil advocate' as a verb instead of its conventional mode or function a noun. The flipping the role of the phrase from a noun to a verb, i.e. innovating a new usage of the phrase 'devil advocate', for example, is essential linguistic manoeuvring which enables a comprehensive and sharp comparison of the similarities between two groups of Nigerians: cybercriminals and the law-abiding citizens. This contribution is new in cybercrime scholarship about Nigeria. ➢ The first conceptual publication on cybercrime to 'devil advocate' the 'sainthood' of claimed law-abiding citizens, by highlighting that the line dividing them and the Nigerian cybercriminals (Yahoo-Boys) is blurred with regards to the use of magical means for material ends. Unlike prior research, the article casts a brighter light on the line dividing cybercriminals and law-abiding citizens with respect to the use of spiritual and magical power for material gains. ➢ The first publication which explored the occult economy in a variety of different manifestations, namely (1) the traditional African spiritual system; (2) the Olokun deity; (3) the Gospel of Prosperity; and (4) the villagization of the modern public sphere, to unpack the ways in which local epistemologies and worldviews on wealth acquisition give rise

	to contemporary manifestations of spirituality in cyberspace. ➢ By underlining that contextual realities on the ground should be taken seriously, beyond their particular geographical and disciplinary contexts, the article underscored the idea that cultural realities should inform policymaking in the real world of a spiritually embedded economy in a Nigerian context. In particular, it is the first publication to identify that the concept of escapelessness has cybersecurity benefits (because legitimacy and conformity to social rules are central to self-regulation, e.g. Tyler, 1990). By implication, it is also the first publication to construct the connection between 'digital spiritualization' and the concept of escapelessness. ➢ The article concludes that if people believe that all aspects of life are reflective of the spiritual world and determined by it, the spiritual realm, by implication, is the base of society, upon which sits the superstructure comprised of all aspects of life, especially wealth. This conceptual position is the first to point out that, inferentially, the idea that the spirit world is the base of the Nigerian society is an inversion of Orthodox Marxist theory of economic determinism.
Ibrahim (2016a)	➢ The first publication to deconstruct a number of dominant taxonomies used in cybercrime scholarship (e.g. 'the binary model of cybercrime'). By doing so, the research also critiqued the meaning of the term 'cybercrime' and redefined it. ➢ The first peer-reviewed research to develop the Tripartite Cybercrime Framework (TCF) which is a more conceptually robust framework for examining cybercrime in a Nigerian context (and elsewhere). The TCF proposed that

	cybercrime can be motivated in three possible ways: socioeconomic, psychosocial and geopolitical, which is new in cybercrime scholarship. ➢ The first publication to use the synergy between motivational theories and the basic psychological framework of categorisation, to classify cybercrime types. ➢ The first publication to illustrate that whilst in Nigeria, cybercrime is fundamentally rooted in socioeconomics, the lenses of the existing cybercrime taxonomies are not well equipped to clearly project the pattern of this phenomenon. ➢ The first publication to demonstrate that the conceptual 'pipelines' of the cybercrime framework in the Global North cannot hold water in Nigeria (Global South). ➢ The first piece of research to critique and challenge the dominant statistics relied on to inform the prevalence of cybercrime perpetrators across nations (e.g. the Internet Crime Complaint Centre's 2010 data set, i.e. IC3 2010). The IC3's (2010) report, for example, has previously misled some authors (e.g. Aransiola & Asindemade, 2011; Chawki et al., 2015) to uncritically represent the statistics about Nigeria. ➢ The first publication to illuminate that the populist view that cyber-fraud makes Nigeria a global cybercrime player is misplaced because cybercrime has tripartite groups and Nigeria is only relevant in one category – that of socioeconomic cybercrime. Thus, it provides a clearer conceptualisation of cybercrime about Nigeria (and elsewhere).

Lazarus (2019b)	➢ The first peer-reviewed work to build synergy between the feminist epistemology of crime and the Tripartite Cybercrime Framework. ➢ The publication contributed to feminist criminological accounts of digital crimes and victimizations like other articles published before it (e.g. Jane, 2014; Powell & Sugiura, 2018). However, the publication is the first piece of research to advocate the centrality of gender as a theoretical entry point for the investigating of digital crimes by exploring the synergy between the feminist criminology and the Tripartite Cybercrime Framework. ➢ The research critiqued the meaning of the term 'cybercrime' and redefined it by sharpening the contrasts between the socioeconomic and psychosocial categories and drawing from many social contexts, including Nigeria. ➢ The publication critiqued the General Theory of Crime (GTC) by comparing three digital crimes framed with the GTC (a case study). This critique helped to highlight theoretical and methodological pitfalls in using this the GTC in examining cybercrime types (instead of the synergy between the feminist criminology and the Tripartite Cybercrime Framework). It also illustrated the real-life repercussions of this type of theoretical and methodological oversights in research. ➢ It concluded that who is victimised, why, and to what effect do not apply in the same way to socioeconomic cyber-crimes as they do to psychosocial cybercrimes by relying on the synergy between the feminist criminology and the Tripartite Cybercrime Framework.

Having outlined the arrays of significant contributions to knowledge by the three conceptual publications, I now move on to the rationale for including the empirical studies.

4. **The empirical publications**

4.1.**Rationale for inclusion**

Publication
Ibrahim, Suleman. (2016b). Causes of Socioeconomic Cybercrime in Nigeria. In: IEEE *International Conference on Cybercrime and Computer Forensic* (ICCCF), Vancouver, BC, Canada (pp. 1-9). *IEEE* Publishing.

This publication is included because it uses parents as its sample, whereas, prior studies (e.g. Aransiola & Asindemade, 2011) primarily depended on university students as their samples. This is important because distinct slices of data often yield different perspectives on the subject of inquiry. Additionally, Ibrahim (2015) (an earlier publication excluded from this submission as previously mentioned) contrasted the cultural consequences of parental death and parental divorce. By doing so, it deconstructed the singular model of 'broken-home' in the existing comparative criminology literature and illustrated that familial factors in themselves are a more important index of the rate of criminality in young people in Nigeria than in the West (Ibrahim, 2015). Even though the vulnerability effect of any single familial factor is magnified only in the presence of other factors (e.g. structural factors) (Young, Fitzgibbon & Silverstone, 2014), familial factors are the major determinants of children's behaviour in a Nigerian context due to historical underpinnings (Ibrahim, 2015). Thus, Ibrahim (2016b) which explored parents' perceptions about cyber criminality fits the theme and agenda of this topic of inquiry. Also, like Lazarus (2019a), the reasons for including this publication extend to a new research endeavour. My future research in this area will aim to

recruit/interview Nigerian parents whose son or daughter has officially been criminalised as a cybercriminal. The study, I believe, will help to cast a brighter light on the cultural and social dimensions of cybercrime in a Nigerian context.

Publication
Lazarus, Suleman. (2018). Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists. Criminology, Criminal Justice, Law & Society, 19, (2) 63-81.

First, this publication is included because of its uniqueness in offering a fresh light to the examination of empirical traces of hip-hop culture in cyber-fraud. It urges cyber-fraud researchers to look beyond traditional data sources (e.g. cyber-fraud statistics) for the empirical traces of 'culture in action' that render fraudulent practices acceptable career paths for some Nigerian youths. Second, the study provides access to coded-languages or slangs used in cyber-fraud victimisations. The study of lyrics opens a vital window of opportunity to examine what Mills (1940, p. 905) called the *vocabularies of motive* (see also Kubrin, 2005, p. 366). 'When a singer vocalises a message, he is not simply trying to describe his experienced social action or social environment. He is not also merely stating "reasons". While he is influencing others, he is also influencing himself' (Mills, 1940, p. 906). Thus, Lazarus (2018) shed light on the cultural and social dimensions of cyber-fraud committed by Yahoo Boys either in Nigeria or elsewhere in the world. Last, but not least, Lazarus (2018) fits squarely with the theme and agenda of this submission, because it is the first study to use a naturalistic set of data from music artists as a tool with which the interpretation of conducts by Yahoo Boys and their economic allies proceeds.

Publication
Lazarus, Suleman & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, 40, 14-26.

This publication is included because it involves an underrepresented set of data in cybercrime scholarship. In particular, the study is based on 'a-hard-to-reach' primary dataset, which fits with the theme of the agenda of this research portfolio. While gathering data from law enforcement officers about criminals is consistent with prior research (e.g. Hutchings & Chua, 2017), to date, no one has been able to access such invaluable interviewees directly. The study is also unique because an officer interviewed fellow officers providing insider perspectives resulting in particularly rich data. As a result, Lazarus & Okolorie (2019) has many implications for a range of generally accepted viewpoints about the Nigerian cybercriminals previously taken for granted. The study helps to cast a clearer light, for example, on the findings from Lazarus' (2018) study included in this submission (but not solely).

4.2.**Contributions to knowledge**

Having outlined the rationale for including these three qualitative studies in this submission, I summarise their original contributions to knowledge in Table 6 below.

Table 6. List of original contributions to knowledge (empirical outputs)

Publications	*Key contributions to knowledge in the field*
Ibrahim (2016b)	➢ The study is the first peer-reviewed publication to use a data set derived from Nigerian parents to shed light on cyber-fraud involvement on the part of Nigerian youths. ➢ The study is the first of its kind in a Nigerian context to highlight that a range of familial factors such as 'a good family environment' have more influence on a person's susceptibility to involvement in cybercrime than external factors such as corruption. ➢ On one hand, unlike prior studies primarily based on university students as their samples, the study underscored the significance of familial

	factors when addressing cyber-fraud involvement among Nigerian youths. On the flip side, the study supports a central finding of these prior studies: the centrality of university students and graduates as cyber-fraud perpetrators in a Nigerian context. ➢ The publication revealed that cybercriminals (Yahoo Boys), thugs (Area Boys), and cult members (Cult Boys) are interlinked within Nigerian universities. Since these 'boys' are not likely to stop offending after their graduation, by implication, they may evolve into international organised crime groups (the Federal Bureau of Investigation recently validated this claim, according to a court reporter – Sullivan, 2019). ➢ The study also highlights that a complex web of familial factors and structural forces, alongside cultural forces, explains the degree of cyber-fraud involvement on the part of Nigerian youths. ➢ The study also supports the central arguments of the conceptual publications (Ibrahim, 2016a; Lazarus, 2019a; Lazarus, 2019b): [a] Cybercrime in a Nigerian context is rooted in socioeconomics. [b] Cultural factors and cybercrime are intractably intertwined in a Nigerian context.
Lazarus (2018)	➢ The study is the first publication to identify the ethics of Nigerian cyber-criminals as expressed by music artists. The study academically coined the term 'the ethics of Yahoo Boys', and 'the ethics of Yahoo-Boys can be understood as a set of perceptual alterations that offer them 'psychological shields' to justify their conduct and thus, circumvent self-condemnation' (see Bandura, 1999; Sykes & Matza, 1957). ➢ The study is the first one of its kind to provide a more in-depth insight into the ways crime and illegal money are represented in hip-hop music.

	➢ The study is the first peer-reviewed publication to draw attention to the ways some cybercriminals and some hip-hop musicians are connected. The recent arrest of Naira Marley, a Nigerian singer, in May 2019 for money cyber-fraud charges validates the significance and contemporaneity of Lazarus (2018). ➢ The study provides a unique insight into victim-criminal relations. The publication shed light on the relationship between cybercriminals and their victims, not from victims' narratives (as most victim-oriented studies in the scholarship), but from an underrepresented set of data – lyric data, and lyrical depictions of victims in Nigerian hip-hop music. ➢ The study is also the first of its kind to expose the presence of the mechanisms of moral disengagement (Bandura, 1999) and neutralisation techniques (Sykes & Matza, 1957) in cyber-fraud victimization in a Nigerian context. ➢ The article also provides a comprehensive analysis of the linguistic significance of the word, 'maga' in cyber-fraud victimisation. The publication is indeed the first empirical data to argue that the 'maga' used in cyber-fraud contexts has metamorphosed from the term 'mgbada', which is a game animal – an antelope. ➢ The article is the first peer-reviewed publication to identify that the indigenous language used by some high-profile, educated fraudsters has facilitated the entry of 'mgbada' into the 'yahoo-yahoo' (cyber-fraud) vocabulary. The deployment of this coined word (from 'mgbada' to 'maga') is particularly significant as it sheds light on the perpetrator-victim relationship as that of a hunter and their game-animals (prey). The making of knowledge here is significant. The word 'maga', not only has a unique origin, but it

	also has no precise counterparts. Decoding the term 'maga' facilitated new ways of seeing previously invisible relationships between the 'hunters' and their 'game-animals' all over the world. ➢ Like Ibrahim (2016b), the study also supports the central arguments of the conceptual publications (Ibrahim, 2016a; Lazarus, 2019a; Lazarus, 2019b), that [a] Cybercrime in a Nigerian context is rooted in socioeconomics. [b] Cultural factors and cybercrime are intractably interconnected in a Nigerian context.
Lazarus & Okolorie (2019)	➢ The study is the first peer-reviewed publication to explore the narratives of officers who have close interactions with the Nigerian cybercriminals even though frontline law enforcement officers who routinely investigate, arrest, interview, interrogate and prosecute these cyber-fraudsters have insiders' insights. Thus, it is the first of its kind study to use the narratives of the Economic and Financial Crimes Commission (EFCC) frontline agents (or law enforcement officers for that matter) concerning the Nigerian cybercriminals. ➢ The study is also the first study to bifurcate the Nigerian cybercriminals and their operations based on three factors: educational-attainment, modus-operandi, and networks-collaborators. This contribution would enable relevant agencies to [a] appreciate the vulnerabilities of their victims to develop more adequate support schemes and [b] develop effective response strategies. ➢ Economic power is the most significant pillar of successful masculinity in Nigeria (e.g. Lazarus et al., 2017). The study shed a brighter light on the actions and features of two groups of men (cybercriminals) in their attempts to fulfil the expected role of provider – girlfriends, wives, children.

	➢ Like Ibrahim (2016b) and Lazarus (2018), the study also supports the central arguments of the conceptual publications (Ibrahim, 2016a; Lazarus, 2019a; Lazarus, 2019b) that [a] cybercrime in a Nigerian context is rooted in socioeconomics. [b] Cultural factors and cybercrime are intractably intertwined in a Nigerian context.

5. **Research Significance and Impact**

Making contributions to knowledge is in itself an aspect of research significance and impact (Agozino, 2003; Moed & Halevi, 2015), and all six publications have contributed to knowledge as outlined in Tables 5 & 6 above. Thus, in this section, I focus on different measure of my research significance and impact: [a] citations [b] research utility, and [c] altermetrics. The 'evidence of citations' is a vital aspect of research significance and impact (Nightingale & Marshall, 2013, p. 430-433), and citations matter as much as omissions (Baker, 2019). Citation rates of research, however, are influenced by multiple factors (Milard & Tanguy, 2018; Moed & Halevi, 2015). According to Moed & Halevi (2015), some of these factors are, [a] the popularity of the author in the field; [b] multi-national and multi-authored publication; [c] age of the publication; and [d] the subject area – emerging/specific or established/generalist. First, while three of my publications were published in 2019 (Lazarus 2019a; Lazarus, 2019b; Lazarus & Okolorie, 2019), others are relatively recent (Lazarus, 2018; Ibrahim, 2016a; Ibrahim, 2016b). Second, I am an emerging scholar in the field, and research citation/impact is linked to the author's career stage (see also Balaban, Wróblewska & Benneworth, 2019). Third, none of the publications here involved a co-author excerpt Lazarus & Okolorie (2019). Fourth, the topic of my inquiry is emergent/specific. On all these factors listed above, my citation counts are likely to be suppressed.

In addition to Moed & Halevi's (2015) list, social (dis)advantage, which is inequality in the central and value things people are able to be or achieve (Dean and Platt, 2016) influences citation rates. 'Academia is embedded in prestige economy' (Baker 2019, p.1), whereas there is an absence of insights from Nigerian scholars in global discussions of cyber-fraud (Cross, 2018). In general, historically, the mainstream criminological enterprise is reluctant to take the 'ideas of scholars from colonised African nations unconditionally seriously' (Kalunta-Crumpton & Agozino, 2004, p. 1-4). It is thus conceivable that due to historical and colonial underpinnings, criminological contributions from and about the West are much more valued, and favoured than that of the rest, including Nigeria (Agozino, 2003; Cohen, 1988). Like Moed & Halevi's (2015) list above, this type of social (dis)advantage is unlikely to boost the citation rate of my publication outputs included in this submission.

However, insights from the global North are not more significant than those from the global South since cyber-fraud is a globalised phenomenon as the following research on victims of cyber-fraud highlighted: (Button, Lewis & Tapley, 2009; Button, Lewis & Tapley, 2014; Button et al., 2014; Button & Cross, 2017; De Kimpe et al., 2020; Norris Brookes & Dowell, 2019). Indeed, a local crime in a digital and global age is a global crime with international connections and consequences (Hall, 2013; Hall & Scalia, 2019; Lewis, 2018; Silverstone, 2013). Yet, contrary to the above authors' position (i.e. Button et al., 2014; Hall & Scalia, 2019; Lewis, 2018; Silverstone, 2013), some researchers may still consider my topic of inquiry to be local matters that concern only Nigeria. In light of the above reasons, I argue that the evidence of citations alone is inadequate to illustrate the significance/impact of any publication.

It is, therefore, necessary to widen the parameters for evaluating research significance/impact beyond citation rates (Haunschild et al., 2019; Thelwall, 2018).

Alternative ways are required to paint a complete picture. Indeed, 'just because an article is not receiving citations, it does not mean that it is not being read' and used (Nightingale & Marshall, 2013, p. 431). For instance, Ibrahim (2016b) has only five citations (excluding self-citations) (e.g. Bae, 2017; Changalasetty et al., 2019; Oni, Oni & Joshua, 2019; Tsumura et al., 2018); whereas, on ResearchGate alone, it has been read 6056 times and recommended five times by researchers (see Appendix 1). Peer-recommendations are products of reflective thoughts. Such recommendations are indicative of the perceived value of the publications after reading and contemplation. Thus, I argue that peer-recommendations are additional invaluable representations of the publications' significance and utility in their own right.

The 'utility' of peer-reviewed publications is also evident in altermetrics. Altermetrics refers to impact measures of publications based on the number of mentions in the news, blogs, and peers' reactions on social networking sites such as ResearchGate, Twitter and so on (Haunschild et al., 2019; Maggio, Meyer, & Artino, 2017). In recent years, altermetrics have become valid reflections of a publication's significance and impact (Barnes, 2015; Haunschild et al., 2019; Malone & Burke, 2016; Sugimoto et al., 2017; Thelwall, 2018). Consequently, I have included traces of altermetrics in illustrating the significance and impact of all six publications included in this research portfolio as shown in Table 7. However, I have only used specific examples from three of the publications, because they are the most 'popular' publications (in ascending order of significance): [1] Lazarus, 2019a; [2] Lazarus, 2018; and [3] Ibrahim, 2016a.

Table 7. The significance and impact records of publication outputs

Six-published works	*Recommendations at 'ResearchGate'*	*Invited talk or interview*	*News mentions*	*Google Scholar Citations*
Lazarus (2019a)	1	None	2	5
Ibrahim (2016a)	1	1	6	21
Lazarus (2019b)	3	None	None	3
Ibrahim (2016b)	5	None	2	9
Lazarus (2018)	2	2	6	5
Lazarus & Okolorie (2019)	1	None	None	4

First, Lazarus (2019a) is significant not least because it cast a more critical gaze on the taken-for-granted similarities between cybercriminals and the rest of the Nigerians. Through such a gaze, the article considered cybercriminals not as 'alien' to the body of Nigerian society, but as a disturbing reflection of society or a caricature instead (drawing from Matza & Sykes, 1961, p. 717). The value of this conceptual contribution becomes more apparent when one considers that in criminology in particular, due to historical and colonial reasons, 'theoretical originality' from marginalised voices is very much emergent (Ibrahim, 2015, p. 317; see also Cohen, 1988, p. 172). Apart from the above, the article, despite being new, has started to impact on the academic discourse about our understanding of cyber spiritualism. For example, Orji (2019, p. 5) drawing from Lazarus's (2019a) work elucidated:

[The] *definition* [cyber spiritualism] *however has been subject to criticism because it appears to negatively classify all forms of cyber spiritual activities [i.e. Lazarus, 2019a]. In this regard, it has been argued that "the licit and illicit tapping of spiritual resources for wealth acquisition offline predates the use of this practice online, and clarifies the concept of cyber-spiritualism" [Lazarus, 2019a, p. 2-5]. Therefore, the concept of cyber-spiritualism has been defined as 'the use of magical and spiritual powers in cyberspace for functional purposes (e.g. online job applications or online examinations) or dysfunctional purposes (e.g. online scamming), depending on subscribers' intentions and the circumstances they address'*

[Lazarus, 2019a, p. 2-5] Accordingly, the concept of cyber spiritualism has a dual meaning due to its reflection of legitimate and illegitimate elements [as Lazarus, 2019 argued].

Clearly, Lazarus (2019a) has received a seminal citation as shown above (a citation that views the article as influential to new understanding). But that is not all. It has also received passing citations (i.e. citation amongst several grouped references within a literature review) (e.g. Recio-Román, Recio-Menéndez & Román-González, 2019). Additionally, the publication has enabled Lazarus & Okolorie's study (2019) to extend its literature review and discussions beyond prior parameters and assumptions about cyber spiritualism. Beyond the evidence of citations, Lazarus (2019a) has been mentioned twice in news outlets (see Appendix 2). Because of these news mentions, the significance of the water goddess (*Mami Wata*) analysed in Lazarus (2019a) stimulated a social media discussion: '*Starbucks uses the Mami Water logo to bless their business*' (see Appendix 3). Also, Lazarus (2019a) has been read and used by many people around the world. Within nine months of publication - 27th February to 23rd November 2019 - the article was viewed 3202 times, and downloaded 2360 times (see Appendix 4). The article was published open access free of charge through the Knowledge Unlatched scheme (see Appendix 5), and for the category of articles published within last twelve months, it is the second most downloaded article (see Appendix 6). One of the downloaders/readers, a scholar, has approached me for international research collaboration, and consequently, I have become an affiliate, 'a visiting researcher', at the researcher's university - University of California, Berkeley, to facilitate the research collaboration (see Appendix 7).

Second, while Lazarus (2018) has been cited by some researchers (Offei et al., 2019; Park et al., 2019), reporters have also found the article to be newsworthy[7] (see Table

[7] In social science, less than 5% of journal articles published in 2013 were referenced by news sources by mid-July 2018 (Thelwall 2018).

7). To illustrate, I have been invited/interviewed by two journalists: [a] Thomas Kiebl, an award-winning journalist from the only Austrian music magazine called *The Message* (see Appendix 8A); and [b] Marcus Morey-Halldin from a Swedish radio show called *Algoritmen* (see Appendix 8B). Thomas Kiebl's report following the interview was published in German (Kiebl, 2019); whereas Marcus Morey-Halldin published the summary of the interview on iTunes and Spotify on 19th December 2019 (Morey-Halldin, 2019). The engagement with these music journalists has allowed my research to be accessible to a multitude of music lovers who might not have been interested to read peer-reviewed publications. Relatedly, I have disseminated Lazarus (2018) to a broader range of audiences by publishing its key points in a high quality and widely-read blog, *The Conversation* (see Lazarus, 2019e). This blog, Lazarus (2019e), has now been read by over 5000 people around the world (see Appendix 9).

Third, as with Lazarus (2018), I have disseminated Ibrahim (2016a) to a broader range of audiences by publishing its key arguments in *The Conversation* (Ibrahim, 2017). This way, the article became accessible for people all over the world who might be interested in the topic but may not have access to reading academic articles. Not only has this blog (i.e. Ibrahim, 2017) been downloaded more than 15,000 times across the globe, several other news outlets have also referenced Ibrahim (2016a) (see Appendices 10A & 10B). Furthermore, some Nigerians have shared their views online about the significance of this research and how it relates to their real-life experiences in their search for 'greener pastures', supposedly in the West (see Appendix 11). Some academic researchers have also acknowledged the importance of the publication on social media on their own accords as follows. For example, in 2018, a researcher (@1Jamesl) tweeted about Ibrahim (2016a) as follows (see also Appendix 12): '*Before going deep in my next technical project, I retreated for a moment to remind myself - why do we do what we do in cybersecurity? I found this article as*

a general reminder on Taxonomies of Cyber Crime'. Relatedly, I was invited as a speaker to present Ibrahim (2016a) at the University of Strathclyde (see Appendix 13).

Apart from sparking personal and professional interest, Ibrahim (2016a) has been cited by many researchers (e.g. Adejoh et al., 2019; Camp et al., 2019; Feofilova et al., 2019; Kirillova et al., 2017; Nnanwube, Ani & Ojakorotu, 2019; Osho & Eneche, 2018; Roelofs et al., 2018; Solano & Peinado, 2017; Wisdom et al., 2019). While some of these citations were comparative citations (citation as a benchmark against which to compare a research) (e.g. De Kimpe et al., 2020; Park et al., 2019; Solano & Peinado, 2017), some were positive citations (citation which represents a work in a positive light) (e.g. Camp et al., 2019; Feofilova et al., 2019; Wisdom et al., 2019) and others were passing citations (e.g. Adejoh et al., 2019; Chavez, 2018).

For example, De Kimpe et al. (2020, p. 18) wrote, in our study, 'we selected cybercrimes in which offenders usually have a socio-economic motive, rather than a psychological (e.g. cyberstalking) and/or geopolitical (e.g. cyber terrorism) motive (i.e. categorization as proposed by Ibrahim, 2016a)'. In a similar vein, Solano & Peinado (2017, p. 1) wrote, 'we could only find two publications on the topic that take a similar approach to the study of cybercrime. The first of them is *Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals*' [i.e. Ibrahim, 2016a]. Thus, Ibrahim (2016a) is a foundational article, which serves as a reference point for further contributions. But that is not all. Ibrahim (2016a) is also the second most downloaded article from the last quarter of 2019 to the first quarter of 2020: International Journal of Law, Crime and Justice (see Appendices 14A & 14B). In a nutshell, while the evidence of citations discussed above is revealing, I have elucidated that it requires the presence of other factors to present the significance and impact of my publications in a clearer light.

6. **Conclusion**

The critical narrative has reflected on my life experiences and research philosophy that influenced the six publication outputs in this research portfolio. The critical commentary itself and the peer-reviewed publications themselves constitute significant original contributions and extensions to knowledge as outlined in Tables 5 & 6. To recapitulate, in making their unique contribution to knowledge, the three conceptual publications challenged and deconstructed a number of taken-for-granted concepts, taxonomies, in cybercrime scholarship. The above three publications proved valid conceptual lenses to focus on cybercrime in a Nigerian context. Without a doubt, the development of these multiple new conceptual lenses (Lazarus, 2019a; Ibrahim, 2016a; Lazarus, 2019b) exemplifies my 'contribution to developing theory in the field' as outlined by the University of Portsmouth (2019, p. 1). Equally, this narrative has demonstrated that the conceptual publications are not more significant than the empirical publications, not least because of their distinctiveness (see Table 4). The diverse sources of qualitative data (empirical publications) provide a more fully-developed understanding of cybercrime in the Nigerian context (and elsewhere). All six-published works, while individually making a contribution to knowledge, collectively illuminate how closer attention to Nigerian society aids the understanding of Yahoo Boys, their actions and what constitutes 'cybercrime' in a Nigerian context.

Even though the arrays of contributions of this body of research are reflective of contextual and cultural factors of Nigerian society, as Hall & Scalia (2019), Lewis (2018) and Silverstone (2013) observed, in a digital age, the actions of criminals have global consequences. Thus, the six publications included in this submission have global significance. However, this accompanying commentary acknowledges here that while the significance/impact of these six publications is beginning to gain

traction in public, media and academic discourses, it may take some years before the actual significance/impact becomes more apparent.

Nonetheless, the accompanying commentary has illustrated the validity of the publications on which the award for a PhD by Publication is based: First, the critical narrative has demonstrated that the accompanying outputs upon which this submission for the award is based have been [a] rigorously examined by a set of experts in the multiple fields of study and accepted for publication; [b] published in a public domain; and [c] quality controlled by the University of Portsmouth. Second, the body of work has aligned the overarching research philosophy with the research questions and methodologies across the case studies. Third, this body of work as a whole has been recommended and cited by other researchers (e.g. Adejoh et al., 2019; Camp et al., 2019; Changalasetty et al., 2019; De Kimpe et al., 2020; Offei et al., 2019; Park et al., 2019; Wisdom et al., 2019). Fourth, it has also been read by multiple layers of audiences (e.g. academic researchers, journalists), and sparked professional and personal interest such as the news media (see Appendices 6, 7, 8A, 8B, 9, 10A, 10B, 11, 12, 13, 14A and 14B).

Based on the above points, I believe that the contributions of this research portfolio are significant and impactful. The quality of my independent contributions to knowledge (as set out in the Level 8 Doctoral Descriptor contained in the UK Quality Code for Higher Education, 2014) is not only a characteristic of each individual publication included, but it also a feature of this accompanying narrative itself which pulls the six publications together as a whole. On the basis of the contributions of the peer-reviewed publications (outlined in Tables 5 & 6), the following suggestions may be made:

- The category of cybercrime to which Nigeria is most vulnerable is the socioeconomic cybercrime, whereas cybercrime can be motivated in three possible ways (socioeconomic, psychosocial and geopolitical). By implication, the conceptual 'pipelines' of the cybercrime framework in the Global North may not hold water in Nigeria. Thus, I advocate the centrality of socioeconomics as a conceptual starting point for the investigating of digital crimes committed by Yahoo Boys either in Nigeria or elsewhere in the world (Ibrahim, 2016a).

- Also, the bifurcation of the Nigerian cybercriminals (e.g. with respects to 'educational attainment' and 'networks/collaborations') has implications for understanding the actions and features of the cybercriminals better. These insights, I believe, are invaluable to motivate various agencies in appreciating the vulnerabilities of cyber-fraud victims and developing adequate support schemes (Lazarus & Okolorie, 2019).

- By relying on context as a resource for understanding Nigerian cybercriminals (Yahoo Boys), I urge cyber-fraud researchers to look beyond normal 'scientific evidence' and consider the traces of spiritual manipulations of victims for material gains that are all too often ignored in the global discussions of cyber-fraud (e.g. Lazarus, 2019a).

- By exploring the Nigerian cybercriminals' similarities to the society that produced them, I also urge cyber-fraud researchers to search beyond traditional data sources (e.g. cyber-fraud statistics) for the empirical traces of culture in action that render fraudulent practices acceptable career paths for some Nigerians (e.g. Lazarus, 2018).

References

Adejoh, S. O., Alabi, T. A., Adisa, W. B., & Emezie, N. M. (2019). "Yahoo Boys" Phenomenon in Lagos Metropolis: A Qualitative Investigation. *International Journal of Cyber Criminology*, *13*(1) 1-20.

Agozino, B. (2003). *Counter-Colonial Criminology: A Critique of Imperialist Reason*. London: Pluto.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759-763.

Bae, S. M. (2017). The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review*, *78*, 74-80.

Baker, K. J. (2019). Citations matter. *Women in Higher Education,* retrieved from: https://www.wihe.com/article-details/124/citation-matters/, accessed 30/12/19.

Balaban, C., Wróblewska, M., & Benneworth, P. (2019). Early Career Researchers and Societal Impact: Motivations and Structural Barriers, retrieved from: https://ressh2019.webs.upv.es/wpcontent/uploads/2019/10/ressh_2019_paper_31.pdf, accessed 02/12/2019.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, 3(3), 193–209.

Barnes, C. (2015). The use of altmetrics as a tool for measuring research impact. *Australian Academic & Research Libraries*, *46*(2), 121-134.

Becker, H. S. (1967). *Outsiders: Studies in Sociology of Deviance*. New York: Simon and Schuster Ltd.

Berger, L. & Luckmann, T. (1966). *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Penguin.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. London: Routledge.

Button M. & Tunley M. (2014). Criminal Activity in the Financial Sector. In: Gill M. (eds) *The Handbook of Security* (pp. 427-449). London: Palgrave Macmillan.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand journal of criminology*, *47*(3), 391-408.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36-54.

Button, M., Lewis, C., & Tapley, J. (2009). Support for the victims of fraud: An assessment of the current infrastructure in England and Wales, retrieved from: https://researchportal.port.ac.uk/portal/files/1926164/support-for-victims-of-fraud.pdf, accessed 11/11/19.

Camp, L. J., Grobler, M., Jang-Jaccard, J., Probst, C., Renaud, K., & Watters, P. (2019). Measuring Human Resilience in the Face of the Global Epidemiology of Cyber Attacks. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp.4763-4772). HICSS Publishing.

Changalasetty, S. B., Belgacem, B., Badawy, A. S., Ghribi, W., Ahmed, A. M., Bangali, H. & Pemula, R. (2019). Assessing the Relation between Family Background and Juvenile Delinquency using Data Mining. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-4). IEEE Publishing.

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). 419 scam: An evaluation of cybercrime and criminal code in Nigeria. In Chawki M., Darwish A., Khan M.A., Tyagi S (eds) *Cybercrime, digital forensics and jurisdiction* (pp. 129-144). Berlin: Springer International Publishing.

Chavez, N. M., (2018). "Can We Learn from Hackers to Protect Victims?" Electronic Theses, Projects, and Dissertations. 690. Retrieved from: https://scholarworks.lib.csusb.edu/etd/690, accessed 03/12/19.

Cohen, S. (1972). *Folk devils and moral panics*. London: MacGibbon & Kee Ltd.

Cohen, S. (1988). *Against Criminology*. New Brunswick: Transaction.

Cross, C. (2018). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott & M. Sozzo (eds) *The Palgrave Handbook of Criminology and the Global South (pp. 261-280)*. Cham: Palgrave Macmillan.

Dean, H. & Platt, L., (2016). *Social advantage and disadvantage*. Oxford: Oxford University Press.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, 106310, 1-38.

Ellis, S. (2016). *This Present Darkness: A History of Nigerian Organized Crime*. Oxford: Oxford University Press.

Fazlıoğulları, O. (2012). Scientific research paradigms in social sciences. *International Journal of Educational Policies*, *6*(1), 41-55.

Feofilova, T., Radygin, E., Alekseeva, J. & Ivanov, F. (2019). Economic aspects of national security. In SPBPU: *Proceedings of Peter the Great St. Petersburg Polytechnic University International Scientific Conference on innovations in digital economy*, St. Petersburg, Russia (Article 43, 1–7). New York: Association for Computing Machinery.

Francis, K., Mills, J., Chapman, Y., & Birks, M. (2009). Doctoral dissertations by publication: Building scholarly capacity whilst advancing new knowledge in the discipline of nursing. *Internal Journal of Doctoral Studies*, 4, 97-106.

Frankl, V. (1978). *The Unheard Cry for Meaning*. New York: Simon & Schuster.

Freud, S. (1927). *Civilization, Society and Religions: Group Psychology and the Analysis of the Ego, Future of an Illusion and Civilization and Its Discontents*. New York: Penguin Books Ltd.

Geertz, C. (1973). *The Interpretation of Cultures.* London: Fontana.

Gergen, K. J. & Gergen, M. M. (2012). Social Construction. In L. M. Given (eds) *The SAGE Encyclopedia of Qualitative Research Methods* pp. 1-8). Thousand Oaks, California: SAGE Publications.

Gill, P. & Dolan, G. (2015). Originality and the PhD: what is it and how can it be demonstrated? *Nurse Researcher*. 22, (6) 11-15.

Goyanes, M. (2020). Against dullness: on what it means to be interesting in communication research. *Information, Communication & Society*, *23*(2), 198-215.

Hall, T. (2013). Geographies of the illicit: Globalization and organized crime. *Progress in Human Geography*, *37*(3), 366-385.

Hall, T., & Scalia, V. (2019). Thinking through global crime and its agendas. In Hall, T., & Scalia, V. (Eds.). (2019). *A Research Agenda for Global Crime*. Northampton: Edward Elgar Publishing.

Haunschild, R., Leydesdorff, L., Bornmann, L., Hellsten, I., & Marx, W. (2019). Does the public discuss other topics on climate change than researchers? A comparison of explorative networks based on author keywords and hashtags. *Journal of Informetrics*, *13*(2), 695-707.

Hearsum, P. (2015). *Media representations of the deaths of contemporary popular musicians (1993-2012)* (Doctoral dissertation, University of Brighton).

Hutchings, A. & Chua, Y. (2017). Gendering cybercrime T.J. Holt (eds), *Cybercrime through an Interdisciplinary Lens* (pp.167-188). New York: Routledge.

Ibrahim, S. (2015). A Binary Model of Broken Home: Parental Death-Divorce Hypothesis of Male Juvenile Delinquency in Nigeria and Ghana. In S. R. Maxwell & S. L. Lee (eds) *Contemporary Perspectives in Family Research* (Violence and Crime in the Family: Patterns, Causes, and Consequences pp. 311-340). New York: Emerald Group Publishing Limited.

Ibrahim, S. (2016a). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44-57.

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In IEEE *International Conference on Cybercrime and Computer Forensic* (ICCCF), Vancouver, BC, Canada (pp. 1–9). IEEE Publishing.

Ibrahim, S. (2017). The view that '419' makes Nigeria a global cybercrime player is misplaced. *The Conversation*, retrieved from: https://theconversation.com/the-view-that-419-makes-nigeria-a-global-cybercrime-player-is-misplaced-73791, accessed 18/11/19.

Ibrahim, S., & Komulainen, S. (2016). Physical punishment in Ghana and Finland: criminological, sociocultural, human rights and child protection implications. *International Journal of Human Rights and Constitutional Studies*, *4*(1), 54-74.

Internet Crime Centre Complaint Centre (IC3) (2010). 'Internet Crime Report', retrieved from: https://pdf.ic3.gov/2010_IC3Report.pdf, accessed 26/10/19.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology,* 1 (1), 1-6.

Jalongo, M. R., Boyer, W., & Ebbeck, M. (2014). Writing for scholarly publication as "Tacit Knowledge": A qualitative focus group study of doctoral students in education. *Early Childhood Education Journal*, 42, 241- 250.

Jane, E. A. (2014). 'Back to the kitchen, cunt': speaking the unspeakable about online misogyny. *Continuum*, *28*(4), 558-570.

Kalunta-Crumpton, A. & Agozino, B. (2004). Introduction. In A. Kalunta-Crumpton & B. Agozino (Eds.), *Pan-African issues in crime and justice*. Hants: Ashgate Publishing.

Kiebl, T. (2019). "Maga Don Pay!" // Wie die „Yahoo Boys" HipHop regieren. *The Message*, retrieved from: https://themessage.at/yahoo-boys-nigeria/, accessed 23/11/19.

Kirillova, E. A., Kurbanov, R. A., Svechnikova, N. V., Zul'fugarzade, T. E. D., & Zenin, S. S. (2017). Problems of fighting crimes on the Internet. *Journal of Advanced Research in Law and Economics*, *8*(3), 25, 849-856.

Kubrin, C. E. (2005). Gangstas, thugs, and hustlas: Identity and the code of the street in rap music. *Social Problems*, 52(3), 360–378.

Lazar, D. (2008). Selected issues in the philosophy of social science. In C. Seale (eds) *Researching Society and Culture* (pp. 7-20). London: SAGE Publications.

Lazarus, S. (2018). Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists. *Criminology, Criminal Justice, Law & Society*, 19, (2), 63-81.

Lazarus, S. (2019a). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, 10, (3), 146, 1-20.

Lazarus, S. (2019b). Just Married: The Synergy between Feminist Criminology and the Tripartite Cybercrime Framework Journal. *International Social Science Journal*, 69, (231), 15-33.

Lazarus, S. (2019c). Betrayals in Academia and a Black Demon from Ephesus. *Wisdom in Education*, *9*(1), 3, 1-5.

Lazarus, S. (2019d). 'Some Animals Are More Equal Than Others': The Hierarchy of Citizenship in Austria. *Laws*, *8*(3), 14, 1-19.

Lazarus, S. (2019e). What Nigerian hip-hop lyrics have to say about the country's Yahoo Boys. *The Conversation*, retrieved from: https://theconversation.com/what-nigerian-hip-hop-lyrics-have-to-say-about-the-countrys-yahoo-boys-100732, accessed 18/11/19.

Lazarus, S. (2020). From the enchanted forest to a PhD by Publication path. Unpublished manuscript.

Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, 40, 14-26.

Lazarus, S., Rush, M., Dibiana, E. T., & Monks, C. P. (2017). Gendered penalties of divorce on remarriage in Nigeria: A qualitative study. *Journal of Comparative Family Studies*, *48*(3), 351-366.

Lee, A., & Kamler, B. (2008). Bringing pedagogy to doctoral publishing. *Teaching in Higher Education*, 13(5), 511- 523.

Lewis, J. S. (2018). Structural Readjustment: Crime, Development, and Repair in the Jamaican Lottery Scam. *Anthropological Quarterly*, *91*(3), 1029-1048.

Maggio, L. A., Meyer, H. S., & Artino, A. R. (2017). Beyond citation rates: a real-time impact analysis of health professions education research using altmetrics. *Academic Medicine*, *92*(10), 1449-1455.

Malone, T., & Burke, S. (2016). Academic librarians' knowledge of bibliometrics and altmetrics. *Evidence Based Library and Information Practice*, *11*(3), 34-49.

Mason, S., & Merga, M. (2018a). Integrating publications in the social science doctoral thesis by publication. *Higher Education Research & Development*, *37*, (7), 1454-1471.

Mason, S., & Merga, M. (2018b). A current view of the thesis by publication in the humanities and social sciences. *International Journal of Doctoral Studies*, 13, 139-154.

Matza, D., & Sykes, G. M. (1961). Juvenile delinquency and subterranean values. *American sociological review*, 26 (5) 712-719.

May, R. (1953) *Man's Search for Himself.* New York: Dell.

McGerty, L. J. (2000). " Nobody Lives Only in Cyberspace": Gendered Subjectivities and Domestic Use of the Internet. *Cyberpsychology, Behavior, and Social Networking*, *3*(5) 895-899.

Milard, B., & Tanguy, L. (2018). Citations in scientific texts: do social relations matter?. *Journal of the Association for Information Science and Technology*, *69*(11), 1380-1395.

Mills, W. (1940). Situated Actions and Vocabularies of Motive. *American Sociological Review*, 5(6) 904-913.

Moed, H. F., & Halevi, G. (2015). Multidimensional assessment of scholarly research impact. *Journal of the Association for Information Science and Technology*, *66*(10), 1988-2002.

Morey-Halldin (2019). Simkortskapning, Yahoo boys och lagar mot deepfakes, *Algoritmen*, retrieved from: https://urplay.se/program/212867-algoritmen-simkortskapning-yahoo-boys-och-lagar-mot-deepfakes, accessed 20/12/19.

Nightingale, J. M., & Marshall, G. (2013). Reprint of "Citation analysis as a measure of article quality, journal influence and individual researcher performance". *Nurse education in practice*, *13*(5), 429-436.

Nin, A. (1975). *The Diary of Anais Nin: 005*, Orlando, Florida: Harcourt Publishers Ltd.

Nnanwube, E. F., Ani, K. J., & Ojakorotu, V. (2019). Emerging issues around cyber crimes in Nigeria. *Ubuntu: Journal of Conflict Transformation*, *8*(1), 55-71.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245.

Offei, M., Andoh-Baidoo, F. K., Ayaburi, E., & Asamoah, D. (2019). Understanding Internet Fraud: Denial of Risk Theory Perspective. In *International Working Conference on Transfer and Diffusion of IT* (pp. 415-424). Cham: Springer.

Oni, S., Berepubo, K. A., Oni, A. A., & Joshua, S. (2019). E-Government and the Challenge of Cybercrime in Nigeria. In *International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 137-142). IEEE publishing.

Orji, U. J. (2019). An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states. *Computer Law & Security Review*, 35(6) 105330, 1-16.

Osho, O., & Eneche, B. M. (2018). Market Dealers or Perpetrators of Cybercrimes? Investigating Cybercriminal Activities in Information Technology Markets in Nigeria. *i-Manager's Journal on Information Technology*, *8*(1), 11-19.

Park, J., Cho, D., Lee, J. K. & Lee, B. (2019). The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status. *ACM Transactions on Management Information Systems*, 10(4), 13, 1-23.

Peacock, S. (2017). The PhD by Publication. *International Journal of Doctoral Studies*, 12, 123-134.

Powell, A., & Sugiura, L. (2018). Resisting rape culture in digital society. In W. S. DeKeseredy, C. M. Rennison, A. K. Hall-Sanchez (eds) *The Routledge International Handbook of Violence Studies* (pp. 447-457). New York: Routledge.

Pycroft, A. (2014). *Addiction and criminal justice interventions: a complex systems analysis* (Doctoral dissertation, University of Portsmouth).

Recio-Román, A., Recio-Menéndez, M., & Román-González, M. V. (2019). Religion and Innovation in Europe: Implications for Product Life-Cycle Management. *Religions*, *10*(10), 589, 1-35.

Roelofs, M., de Koning, N. M., van Vliet, A. J., Wijn, R., Rijk, R. V., & Young, H. J. (2018). *De menselijke kant van Cybersecurity: Conceptuele ontwikkelingen en de Cyber Security Assistent*. Soesterberg: TNO.

Rush, M., & Lazarus, S. (2018). 'Troubling' Chastisement: A Comparative Historical Analysis of Child Punishment in Ghana and Ireland. *Sociological Research Online*, 23 (1),177-196.

Schwandt, T. A (1998). Constructionist, interpretivist approaches to human inquiry. In N. K. Denzin & Y. S. Lincoln (eds) *The Landscape of Qualitative Research: Theories and Issues* (pp. 221 259). Thousand Oaks: SAGE Publications.

Silverstone D. (2013). Globalisation and criminology: The case of organised crime in Britain Globalisation and the Challenge to Criminology in F. Pakes (eds) *Globalisation and the Challenge to Criminology* (pp.27-45). London: Routledge.

Solano, P. C., & Peinado, A. J. R. (2017). Socio-economic factors in cybercrime: Statistical study of the relation between socio-economic factors and cybercrime. In *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1-4). IEEE publishing.

Soule, D. P. (2007). Introducing Writing for Scholarly Journals. In Soule, D. P., Whiteley, L., & McIntosh, S. (eds) *Writing for Scholarly Journals. Publishing in the Arts, Humanities and Social Sciences* (pp.6-9), Glasgow: University of Glasgow Press.

Sugimoto, C. R., Work, S., Larivière, V., & Haustein, S. (2017). Scholarly use of social media and altmetrics: A review of the literature. *Journal of the Association for Information Science and Technology*, *68*(9), 2037-2062.

Sugiura, L. (2016). *Respectable Deviance? Negotiating the opportunities and risks in online medicine purchasing* (Doctoral dissertation, University of Southampton).

Sugiura, L. (2018). *Respectable Deviance and Online Medicine Purchasing: Opportunities and Risks for Consumers*. Basingstoke: Palgrave Pivot.

Sugiura, L., Wiles, R., & Pope, C. (2017). Ethical challenges in online research: public/private perceptions. *Research Ethics*, *13*(3-4), 184-199.

Sullivan, D. (2019). A Tampa fraud case helped reveal the Black Axe, a scheme from Nigeria. *Tampa Bay Times*, retrieved from: https://www.tampabay.com/news/crime/2019/11/11/a-tampa-fraud-cause-helped-reveal-the-black-axe-a-scheme-from-nigeria/, accessed 18/11/19.

Starrs, B. (2008). Publish and graduate? Earning a PhD by published papers in Australia. *M/C Journal*, 11(4), 1-3.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Tannenbaum, F. (1938). *Crime and the Community*. New York: Colombia University Press.

Thelwall, M. (2018). Altmetric Prevalence in the Social Sciences, Arts and Humanities: Where are the Online Discussions?. *Journal of Altmetrics*, *1*(1), 4, 1-12.

The UK Quality Code for Higher Education (2014). 'The Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies', retrieved from: https://www.qaa.ac.uk/docs/qaa/quality-code/qualifications-frameworks.pdf?sfvrsn=170af781_16, accessed 11/10/19.

The University of Portsmouth (2019). "AWARD OF PHD BY PUBLICATION GUIDANCE NOTES", retrieved from: http://www2.port.ac.uk/departments/services/academicregistry/qmd/research

degrees/usefulinformation/RDRegulationsPoliciesandDocumentation/filetodownload,188664,en.docx, accessed 04/10/19.

Thomas, W. I., (1923). *The Unadjusted girl*. Boston: Little Brown and Company.

Thomas, W. I. and Thomas, D. S. (1928). *The Child in America: Behaviour Problems and Programmes.* New York: Alfred Knopf.

Tsumura, H., Kanda, H., Sugaya, N., Tsuboi, S., Fukuda, M., & Takahashi, K. (2018). Problematic Internet Use and Its Relationship with Psychological Distress, Insomnia, and Alcoholism Among Schoolteachers in Japan. *Cyberpsychology, Behavior, and Social Networking*, *21* (12), 788-796.

Tyler, T. (1990). *Why People Obey the Law: Procedural Justice, Legitimacy, and Compliance.* New Haven: Yale University Press.

Wall D.S. (2012). The Devil Drives a Lada: The Social Construction of Hackers as Cybercriminals. In: Gregoriou C. (eds) *Constructing Crime* (pp. 4-18). London: Palgrave Macmillan.

Wilkinson, A. (2015). The rules of the game: A short guide for PhD students and new academics on publishing in academic journals. *Innovations in Education and Teaching International*, 52(1), 99-107.

Wisdom, D.D., Hamza, M. K., Ajayi, E. A., & Odewale, O. O. (2019). Cybercrime: A Threat to a Moral Society. In *International Conference on Education and Development* (pp.364-372). ITED Publishing.

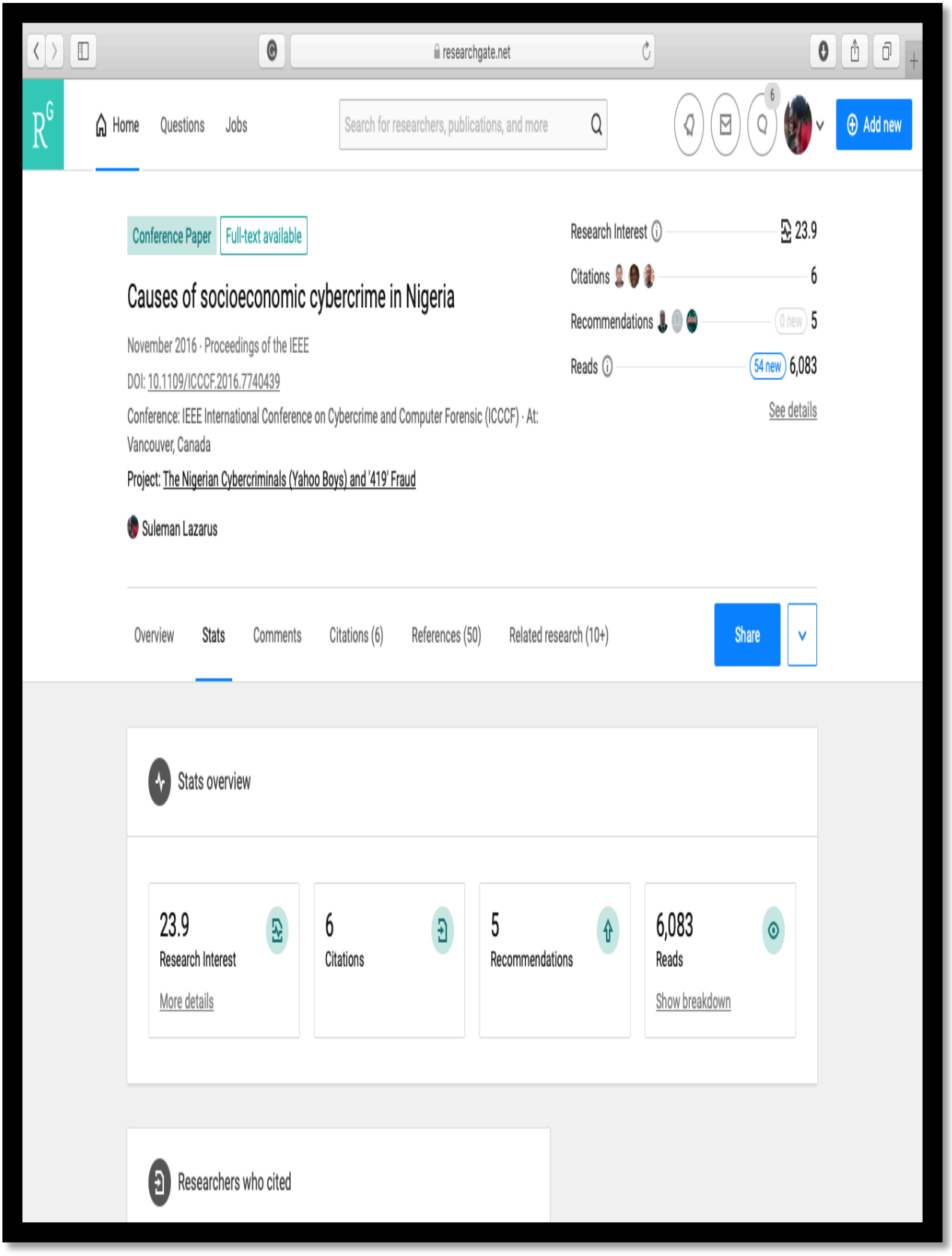
Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society*. London: SAGE Publications Limited.

Young, T., Fitzgibbon, W., & Silverstone, D. (2014). A question of family? Youth and gangs. *Youth Justice*, *14*(2), 171-185.

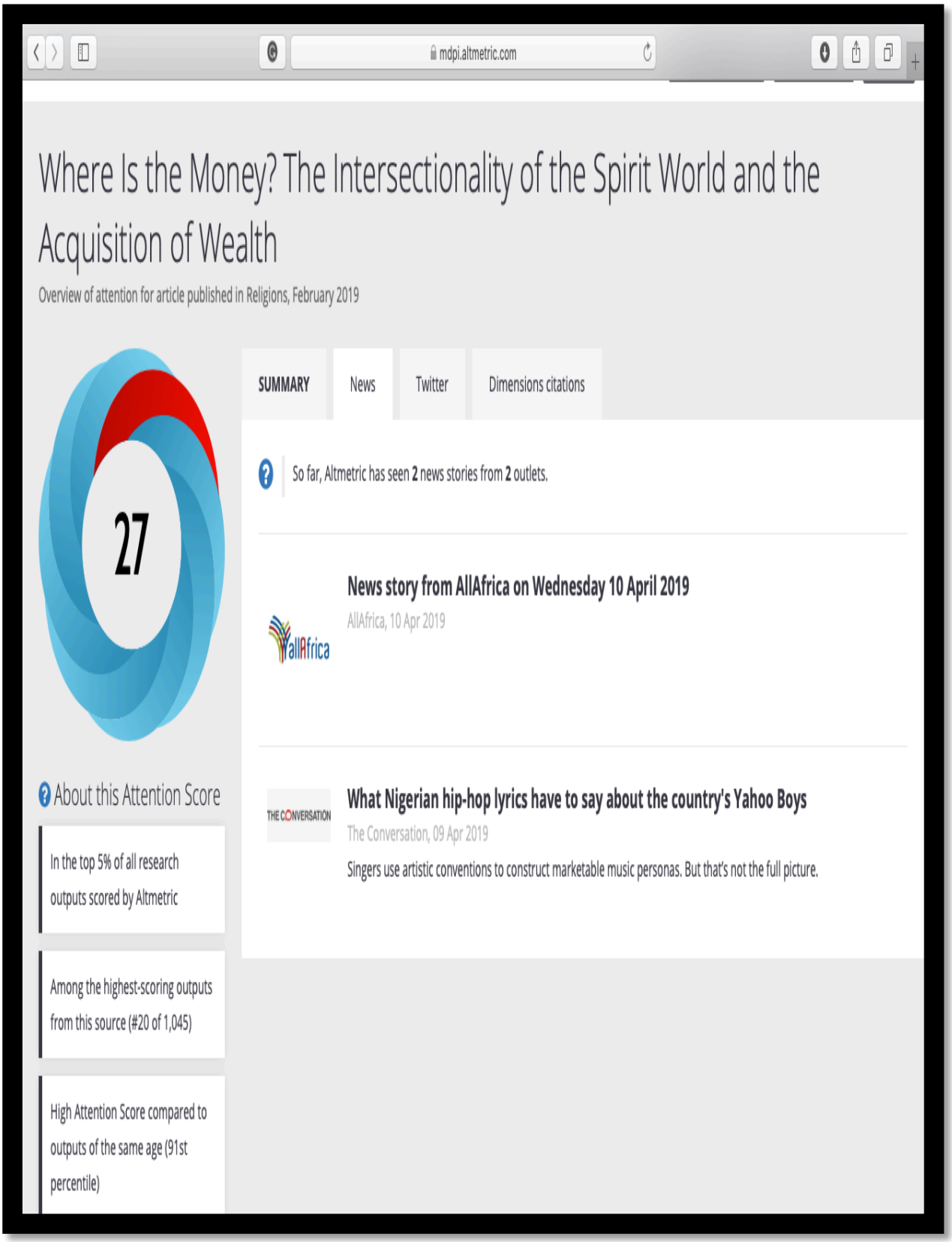
Žukauskas, P., Vveinhardt, J., & Andriukaitienė, R. (2018). Philosophy and Paradigm of Scientific Research. In P. Žukauskas, J. Vveinhardt, & R. Andriukaitienė (eds) *Management Culture and Corporate Social Responsibility (pp. 121-140)*. London: IntechOpen.

Evidence for research significance and impact

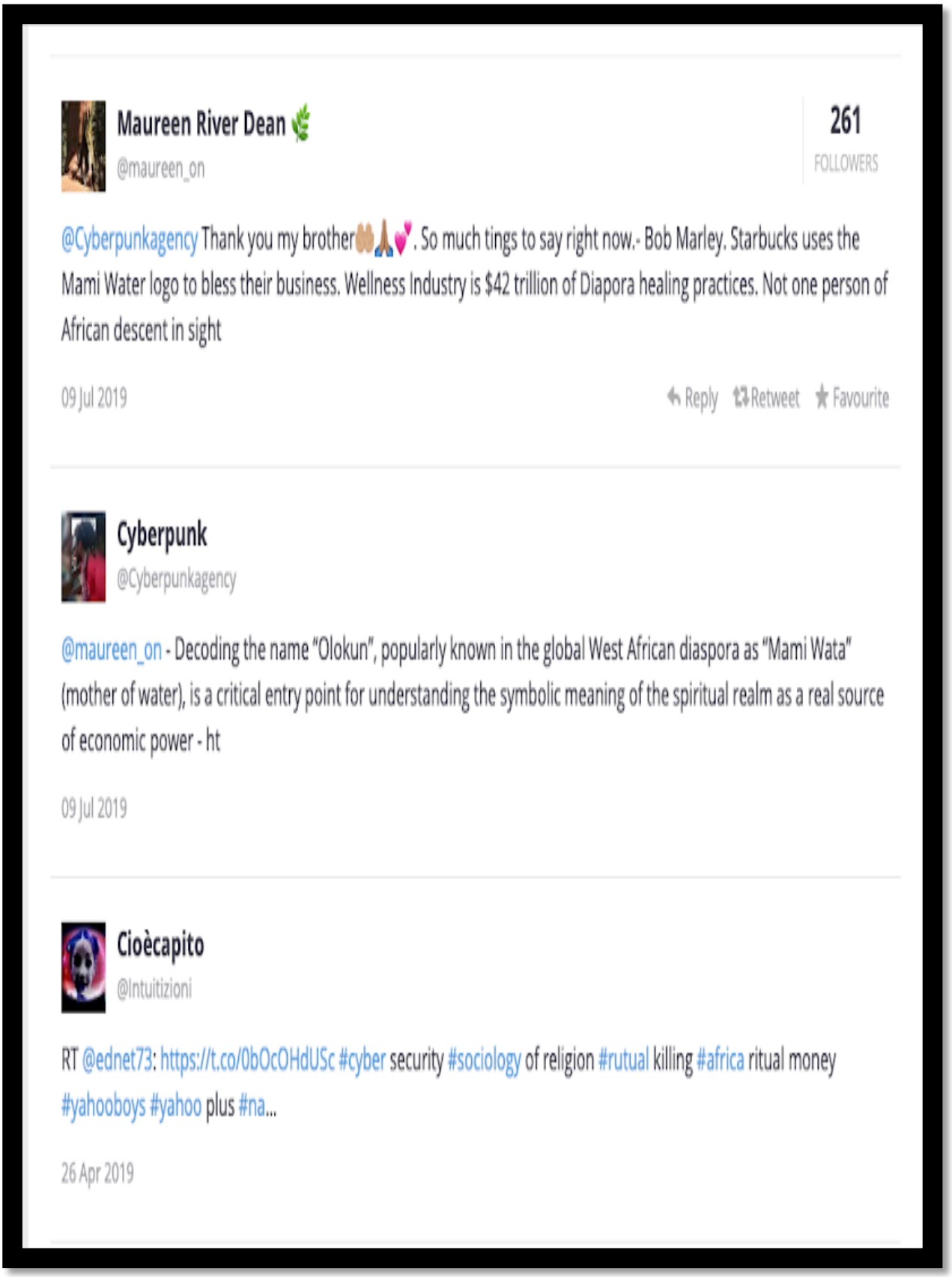
Appendix 1



Appendix 2


mdpi.altmetric.com
Where Is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth
Overview of attention for article published in Religions, February 2019
27
SUMMARY
News
Twitter
Dimensions citations
So far, Altmetric has seen 2 news stories from 2 outlets.
News story from AllAfrica on Wednesday 10 April 2019
AllAfrica, 10 Apr 2019
What Nigerian hip-hop lyrics have to say about the country's Yahoo Boys
The Conversation, 09 Apr 2019
Singers use artistic conventions to construct marketable music personas. But that's not the full picture.
About this Attention Score
In the top 5% of all research outputs scored by Altmetric
Among the highest-scoring outputs from this source (#20 of 1,045)
High Attention Score compared to outputs of the same age (91st percentile)

Appendix 3



Maureen River Dean 🌿
@maureen_on

261
FOLLOWERS

@Cyberpunkagency Thank you my brother🤲🏽🙏🏽💞. So much tings to say right now.- Bob Marley. Starbucks uses the Mami Water logo to bless their business. Wellness Industry is $42 trillion of Diapora healing practices. Not one person of African descent in sight

09 Jul 2019

Reply Retweet Favourite

Cyberpunk
@Cyberpunkagency

@maureen_on - Decoding the name "Olokun", popularly known in the global West African diaspora as "Mami Wata" (mother of water), is a critical entry point for understanding the symbolic meaning of the spiritual realm as a real source of economic power - ht

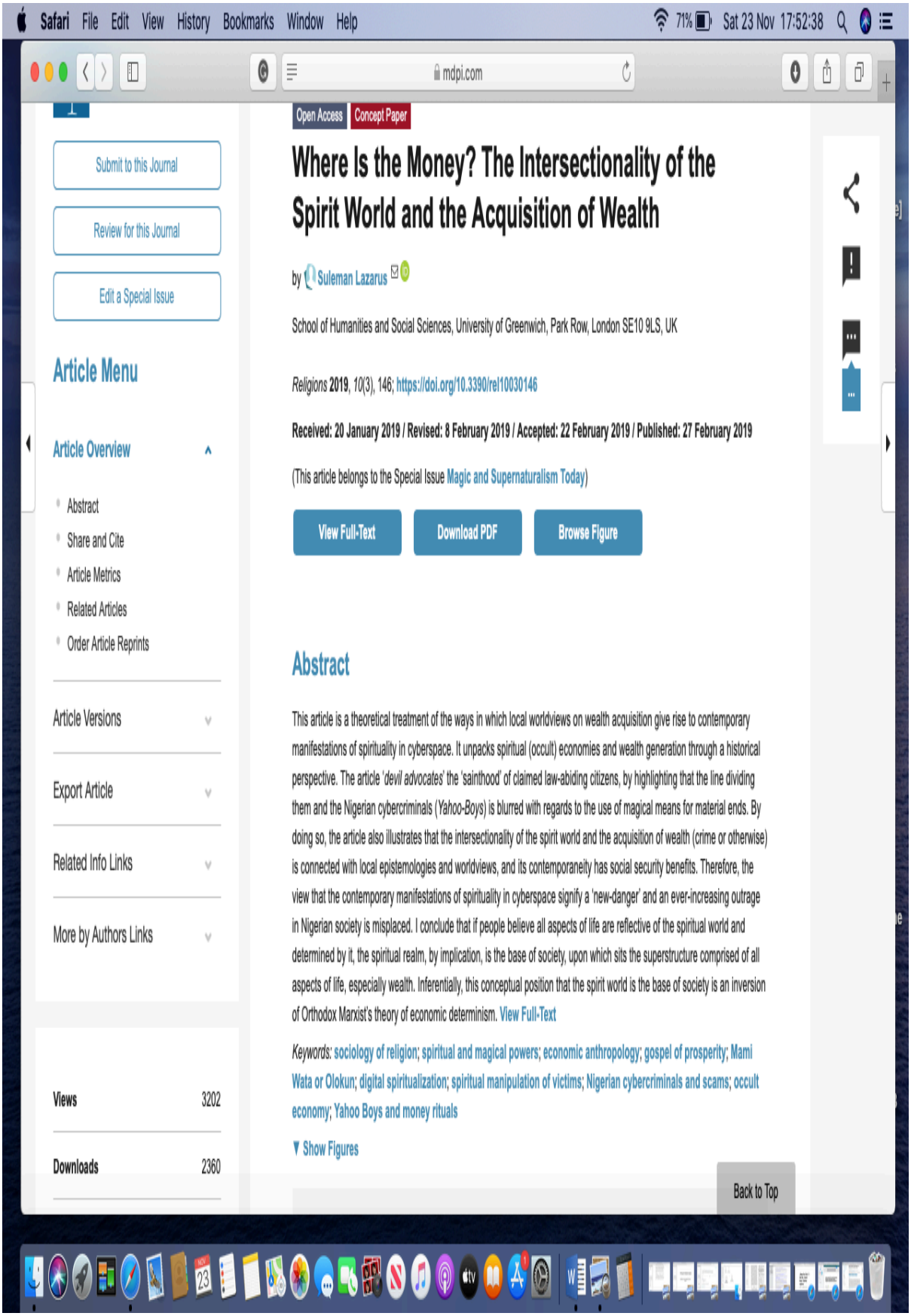
09 Jul 2019

Cioècapito
@Intuitizioni

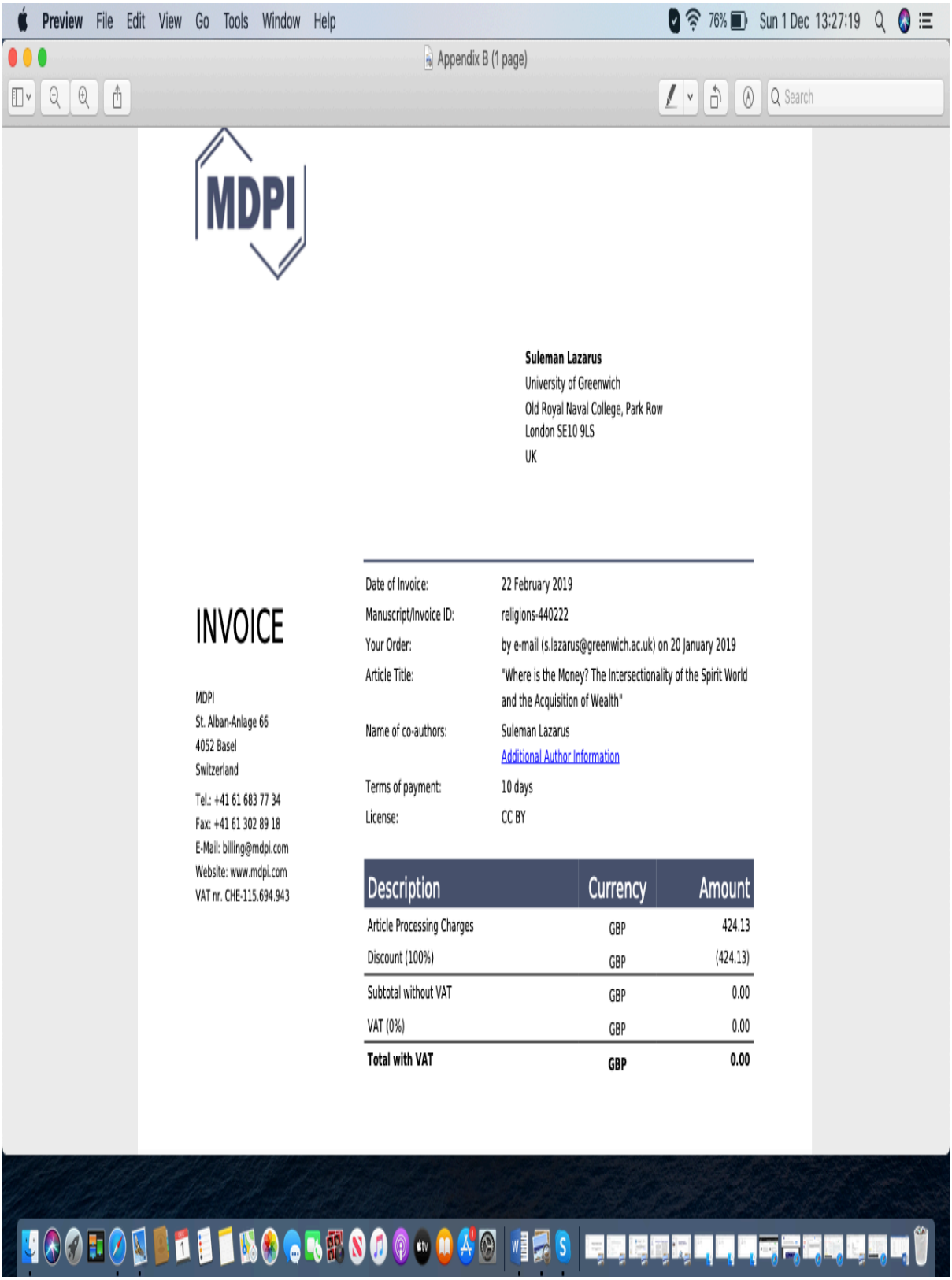
RT @ednet73: https://t.co/0bOcOHdUSc #cyber security #sociology of religion #rutual killing #africa ritual money #yahooboys #yahoo plus #na...

26 Apr 2019

Appendix 4


Safari File Edit View History Bookmarks Window Help
71% Sat 23 Nov 17:52:38
mdpi.com
Submit to this Journal
Review for this Journal
Edit a Special Issue
Article Menu
Article Overview
Abstract
Share and Cite
Article Metrics
Related Articles
Order Article Reprints
Article Versions
Export Article
Related Info Links
More by Authors Links
Views 3202
Downloads 2360
Open Access
Concept Paper
Where Is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth
by Suleman Lazarus
School of Humanities and Social Sciences, University of Greenwich, Park Row, London SE10 9LS, UK
Religions 2019, 10(3), 146; https://doi.org/10.3390/rel10030146
Received: 20 January 2019 / Revised: 8 February 2019 / Accepted: 22 February 2019 / Published: 27 February 2019
(This article belongs to the Special Issue Magic and Supernaturalism Today)
View Full-Text
Download PDF
Browse Figure
Abstract
This article is a theoretical treatment of the ways in which local worldviews on wealth acquisition give rise to contemporary manifestations of spirituality in cyberspace. It unpacks spiritual (occult) economies and wealth generation through a historical perspective. The article 'devil advocates' the 'sainthood' of claimed law-abiding citizens, by highlighting that the line dividing them and the Nigerian cybercriminals (Yahoo-Boys) is blurred with regards to the use of magical means for material ends. By doing so, the article also illustrates that the intersectionality of the spirit world and the acquisition of wealth (crime or otherwise) is connected with local epistemologies and worldviews, and its contemporaneity has social security benefits. Therefore, the view that the contemporary manifestations of spirituality in cyberspace signify a 'new-danger' and an ever-increasing outrage in Nigerian society is misplaced. I conclude that if people believe all aspects of life are reflective of the spiritual world and determined by it, the spiritual realm, by implication, is the base of society, upon which sits the superstructure comprised of all aspects of life, especially wealth. Inferentially, this conceptual position that the spirit world is the base of society is an inversion of Orthodox Marxist's theory of economic determinism. View Full-Text
Keywords: sociology of religion; spiritual and magical powers; economic anthropology; gospel of prosperity; Mami Wata or Olokun; digital spiritualization; spiritual manipulation of victims; Nigerian cybercriminals and scams; occult economy; Yahoo Boys and money rituals
▼ Show Figures
Back to Top

Appendix 5



Preview File Edit View Go Tools Window Help 76% Sun 1 Dec 13:27:19

Appendix B (1 page)

Search

MDPI

Suleman Lazarus
University of Greenwich
Old Royal Naval College, Park Row
London SE10 9LS
UK

INVOICE

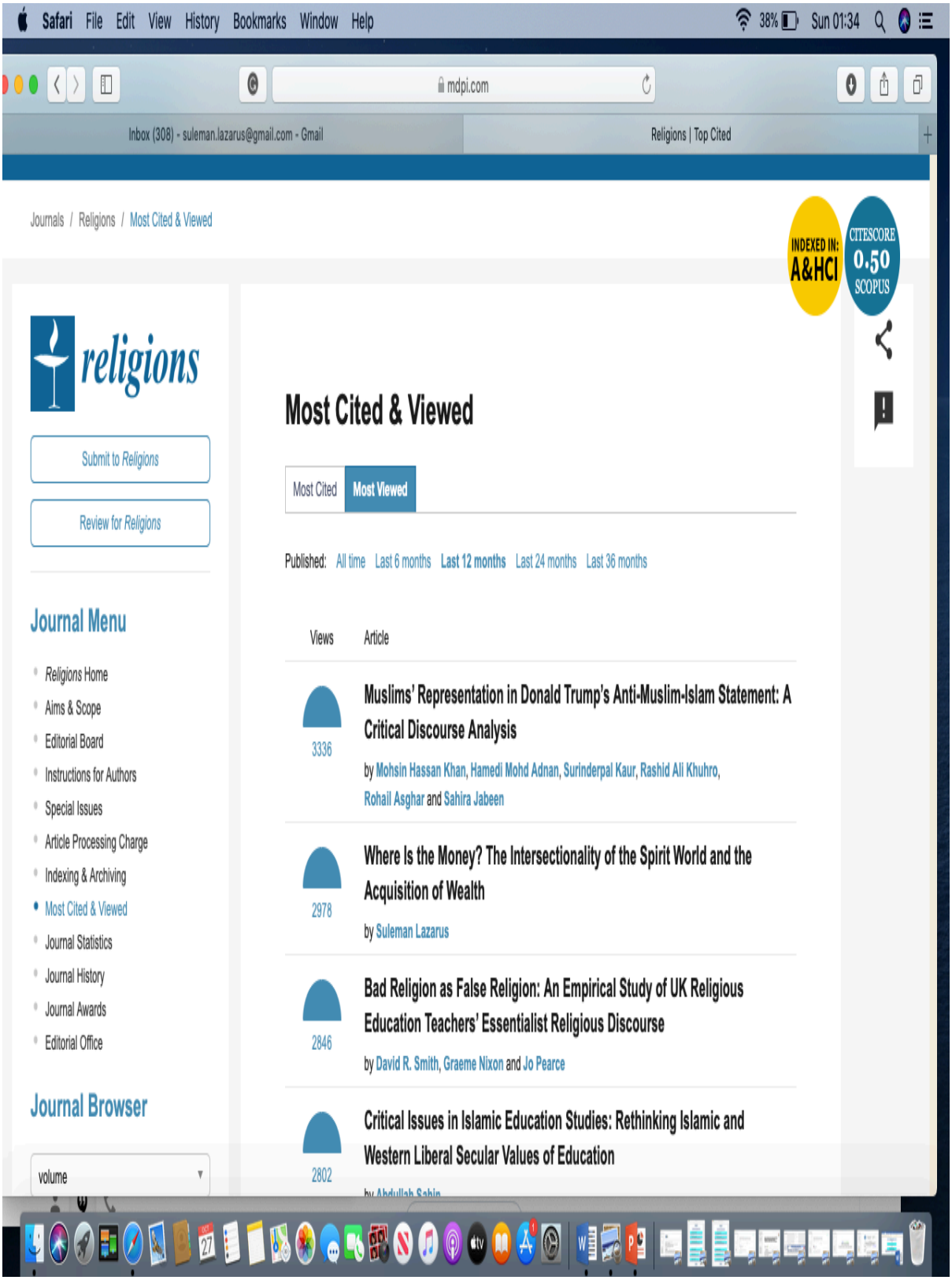
MDPI
St. Alban-Anlage 66
4052 Basel
Switzerland

Tel.: +41 61 683 77 34
Fax: +41 61 302 89 18
E-Mail: billing@mdpi.com
Website: www.mdpi.com
VAT nr. CHE-115.694.943

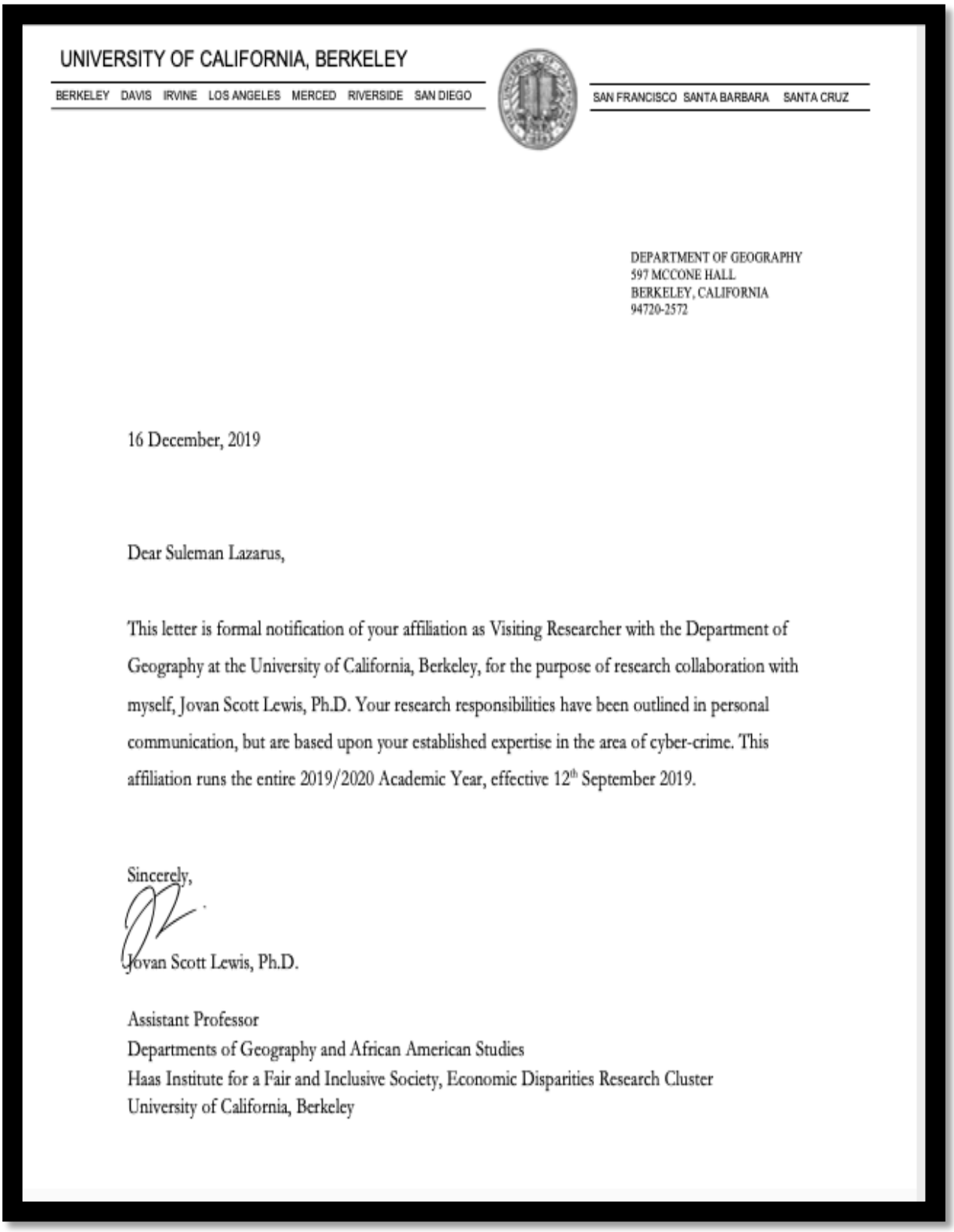
Date of Invoice:	22 February 2019
Manuscript/Invoice ID:	religions-440222
Your Order:	by e-mail (s.lazarus@greenwich.ac.uk) on 20 January 2019
Article Title:	"Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth"
Name of co-authors:	Suleman Lazarus Additional Author Information
Terms of payment:	10 days
License:	CC BY

Description	Currency	Amount
Article Processing Charges	GBP	424.13
Discount (100%)	GBP	(424.13)
Subtotal without VAT	GBP	0.00
VAT (0%)	GBP	0.00
Total with VAT	**GBP**	**0.00**

Appendix 6


Safari File Edit View History Bookmarks Window Help
38% Sun 01:34
mdpi.com
Inbox (308) - suleman.lazarus@gmail.com - Gmail
Religions | Top Cited
Journals / Religions / Most Cited & Viewed
INDEXED IN: A&HCI
CITESCORE 0.50 SCOPUS
religions
Submit to Religions
Review for Religions
Journal Menu
Religions Home
Aims & Scope
Editorial Board
Instructions for Authors
Special Issues
Article Processing Charge
Indexing & Archiving
Most Cited & Viewed
Journal Statistics
Journal History
Journal Awards
Editorial Office
Journal Browser
volume
Most Cited & Viewed
Most Cited
Most Viewed
Published: All time Last 6 months Last 12 months Last 24 months Last 36 months
Views
Article
3336
Muslims' Representation in Donald Trump's Anti-Muslim-Islam Statement: A Critical Discourse Analysis
by Mohsin Hassan Khan, Hamedi Mohd Adnan, Surinderpal Kaur, Rashid Ali Khuhro, Rohail Asghar and Sahira Jabeen
2978
Where Is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth
by Suleman Lazarus
2846
Bad Religion as False Religion: An Empirical Study of UK Religious Education Teachers' Essentialist Religious Discourse
by David R. Smith, Graeme Nixon and Jo Pearce
2802
Critical Issues in Islamic Education Studies: Rethinking Islamic and Western Liberal Secular Values of Education

Appendix 7



UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY DAVIS IRVINE LOS ANGELES MERCED RIVERSIDE SAN DIEGO SAN FRANCISCO SANTA BARBARA SANTA CRUZ

DEPARTMENT OF GEOGRAPHY
597 MCCONE HALL
BERKELEY, CALIFORNIA
94720-2572

16 December, 2019

Dear Suleman Lazarus,

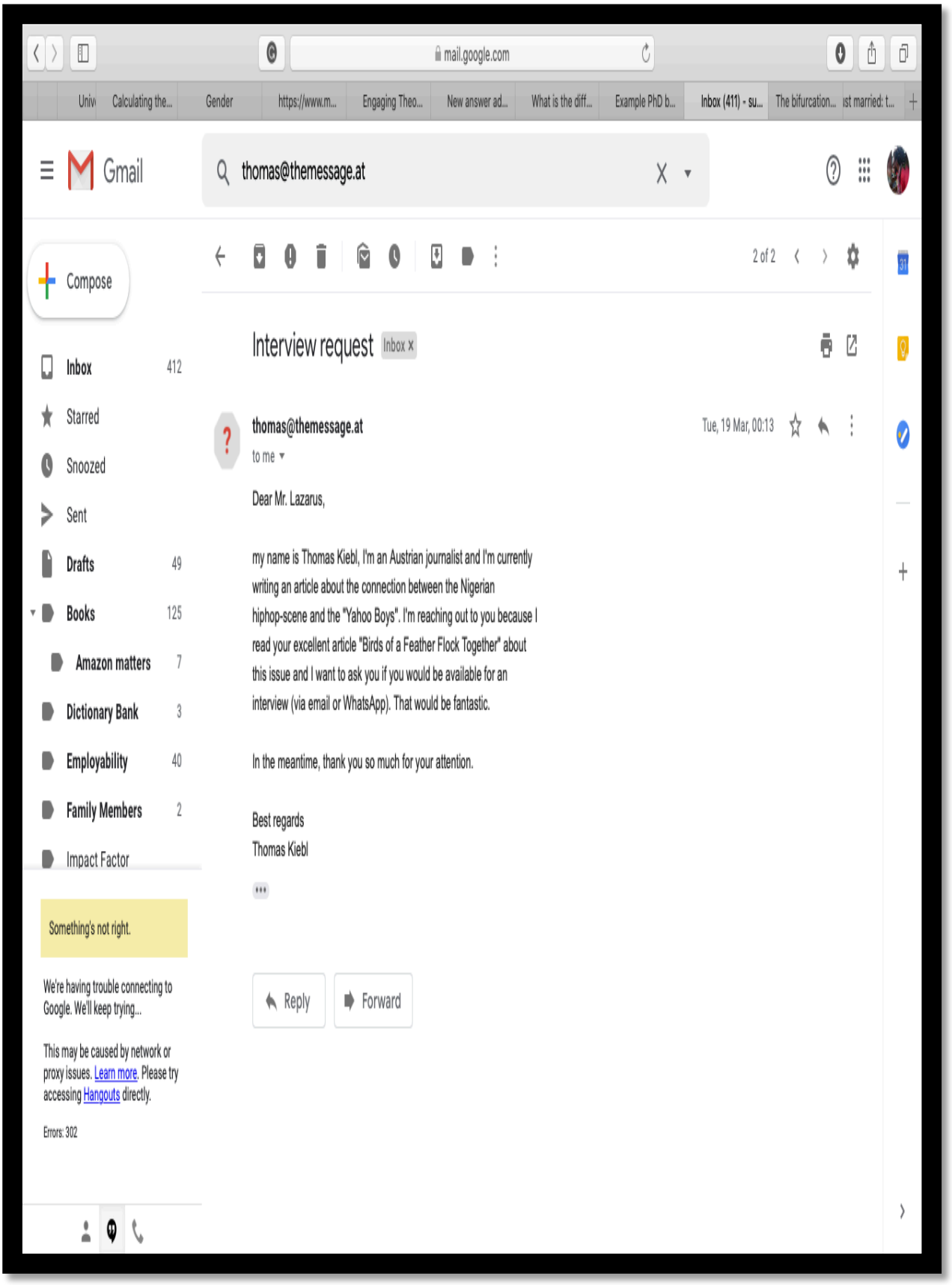
This letter is formal notification of your affiliation as Visiting Researcher with the Department of Geography at the University of California, Berkeley, for the purpose of research collaboration with myself, Jovan Scott Lewis, Ph.D. Your research responsibilities have been outlined in personal communication, but are based upon your established expertise in the area of cyber-crime. This affiliation runs the entire 2019/2020 Academic Year, effective 12th September 2019.

Sincerely,

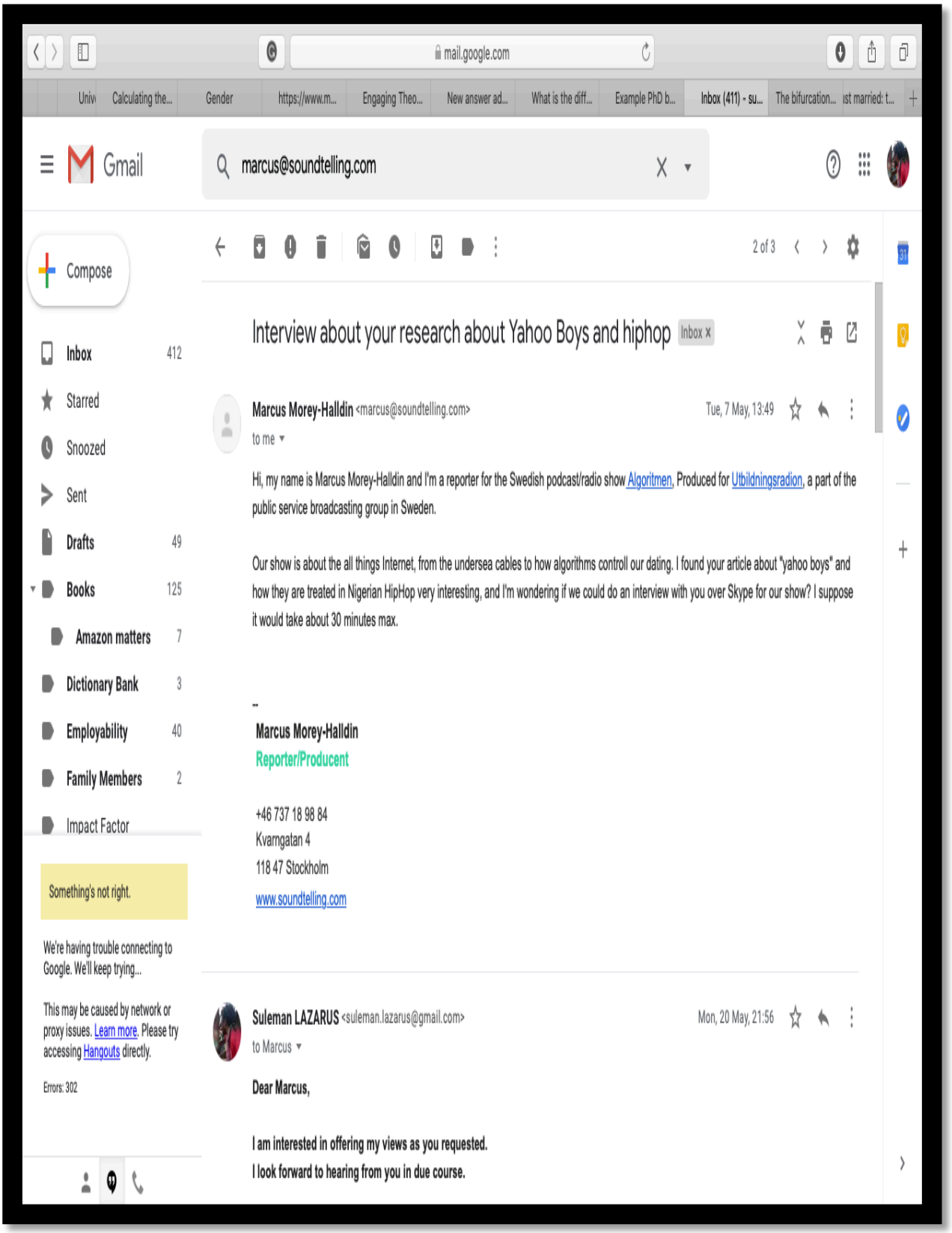
Jovan Scott Lewis, Ph.D.

Assistant Professor
Departments of Geography and African American Studies
Haas Institute for a Fair and Inclusive Society, Economic Disparities Research Cluster
University of California, Berkeley

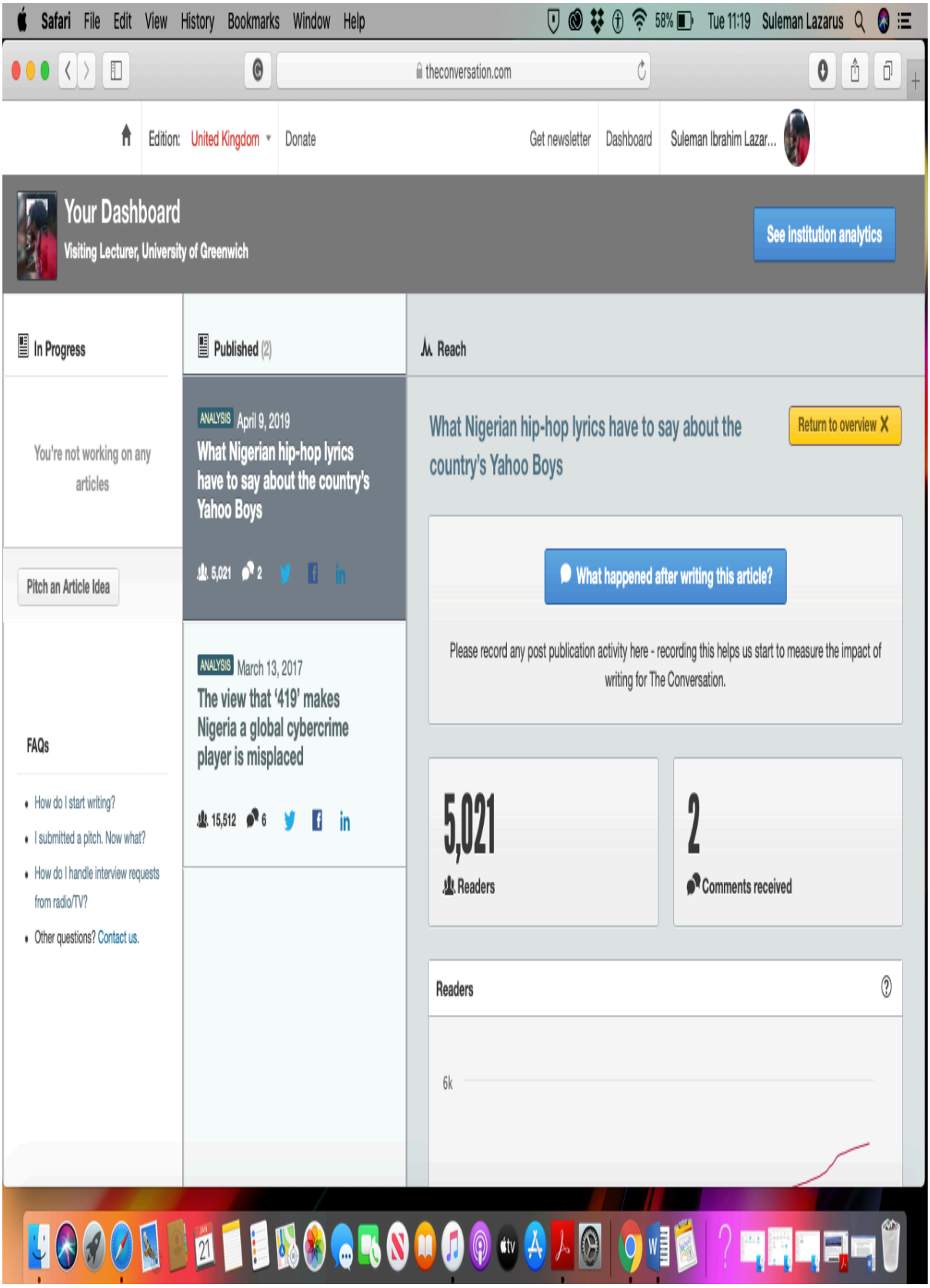
Appendix 8A


mail.google.com
Gmail
thomas@themessage.at
Compose
Inbox 412
Starred
Snoozed
Sent
Drafts 49
Books 125
Amazon matters 7
Dictionary Bank 3
Employability 40
Family Members 2
Impact Factor
Something's not right.
We're having trouble connecting to Google. We'll keep trying...
This may be caused by network or proxy issues. Learn more. Please try accessing Hangouts directly.
Errors: 302
2 of 2
Interview request
Inbox ×
thomas@themessage.at
to me
Tue, 19 Mar, 00:13
Dear Mr. Lazarus,
my name is Thomas Kiebl, I'm an Austrian journalist and I'm currently writing an article about the connection between the Nigerian hiphop-scene and the "Yahoo Boys". I'm reaching out to you because I read your excellent article "Birds of a Feather Flock Together" about this issue and I want to ask you if you would be available for an interview (via email or WhatsApp). That would be fantastic.
In the meantime, thank you so much for your attention.
Best regards
Thomas Kiebl
Reply
Forward

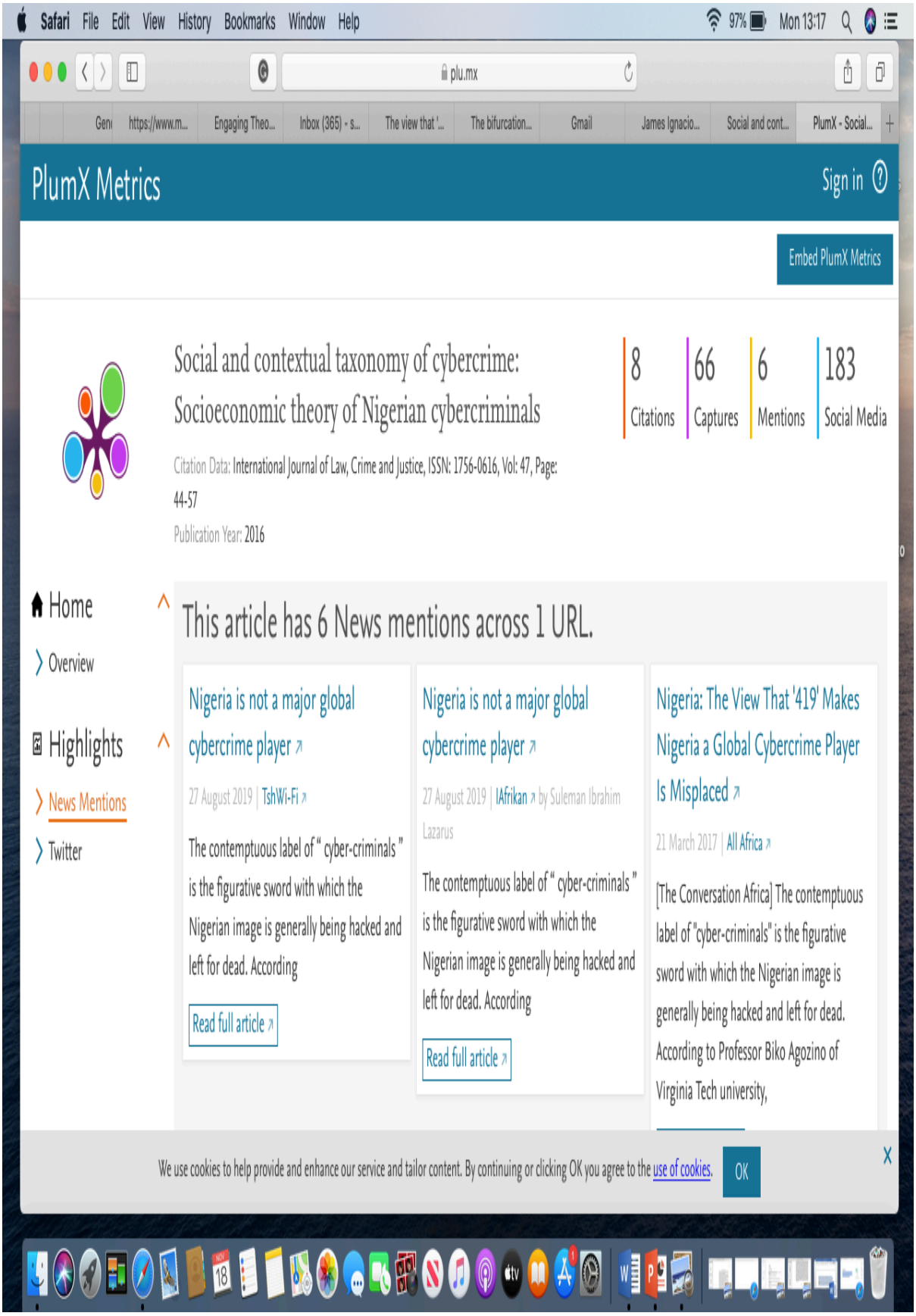
Appendix 8B


mail.google.com
Gmail
marcus@soundtelling.com
Compose
Inbox 412
Starred
Snoozed
Sent
Drafts 49
Books 125
Amazon matters 7
Dictionary Bank 3
Employability 40
Family Members 2
Impact Factor
Something's not right.
We're having trouble connecting to Google. We'll keep trying...
This may be caused by network or proxy issues. Learn more. Please try accessing Hangouts directly.
Errors: 302
2 of 3
Interview about your research about Yahoo Boys and hiphop
Inbox x
Marcus Morey-Halldin <marcus@soundtelling.com>
Tue, 7 May, 13:49
to me
Hi, my name is Marcus Morey-Halldin and I'm a reporter for the Swedish podcast/radio show Algoritmen, Produced for Utbildningsradion, a part of the public service broadcasting group in Sweden.
Our show is about the all things Internet, from the undersea cables to how algorithms controll our dating. I found your article about "yahoo boys" and how they are treated in Nigerian HipHop very interesting, and I'm wondering if we could do an interview with you over Skype for our show? I suppose it would take about 30 minutes max.
--
Marcus Morey-Halldin
Reporter/Producent
+46 737 18 98 84
Kvarngatan 4
118 47 Stockholm
www.soundtelling.com
Suleman LAZARUS <suleman.lazarus@gmail.com>
Mon, 20 May, 21:56
to Marcus
Dear Marcus,
I am interested in offering my views as you requested.
I look forward to hearing from you in due course.

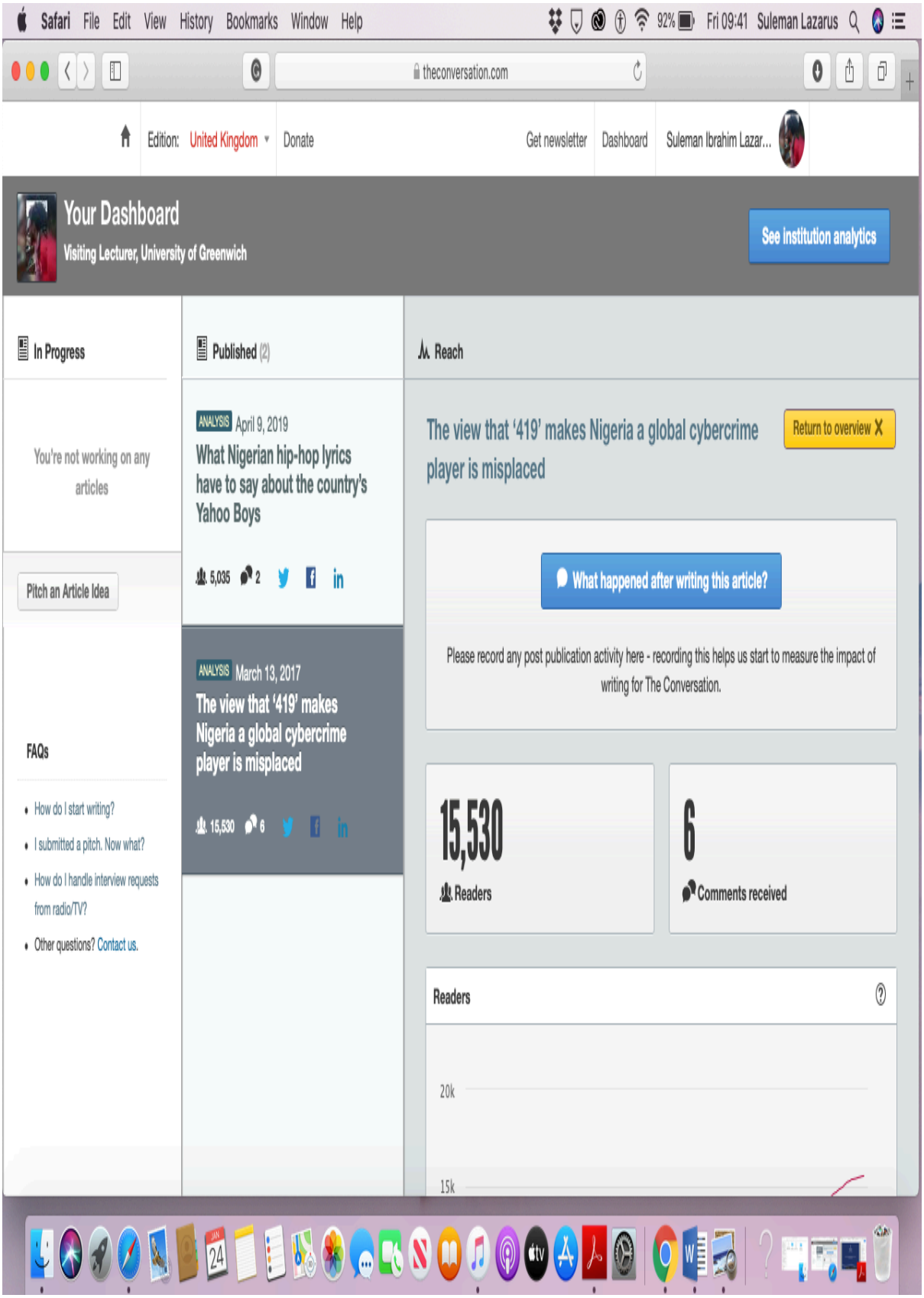
Appendix 9


Safari File Edit View History Bookmarks Window Help
58% Tue 11:19 Suleman Lazarus
theconversation.com
Edition: United Kingdom
Donate
Get newsletter
Dashboard
Suleman Ibrahim Lazar...
Your Dashboard
Visiting Lecturer, University of Greenwich
See institution analytics
In Progress
You're not working on any articles
Pitch an Article Idea
FAQs
How do I start writing?
I submitted a pitch. Now what?
How do I handle interview requests from radio/TV?
Other questions? Contact us.
Published (2)
ANALYSIS April 9, 2019
What Nigerian hip-hop lyrics have to say about the country's Yahoo Boys
5,021 2
ANALYSIS March 13, 2017
The view that '419' makes Nigeria a global cybercrime player is misplaced
15,512 6
Reach
What Nigerian hip-hop lyrics have to say about the country's Yahoo Boys
Return to overview
What happened after writing this article?
Please record any post publication activity here - recording this helps us start to measure the impact of writing for The Conversation.
5,021
Readers
2
Comments received
Readers
6k

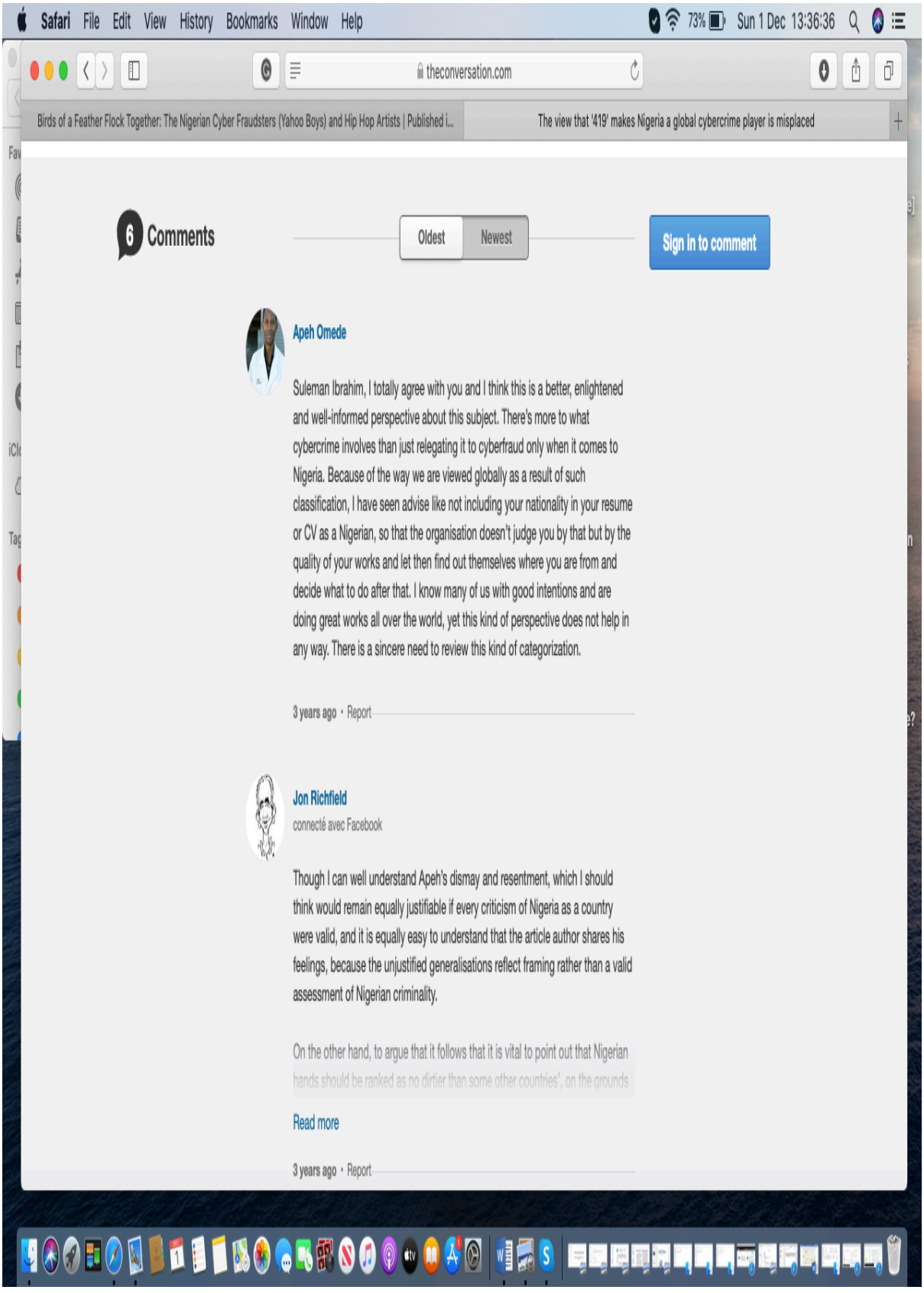
Appendix 10A



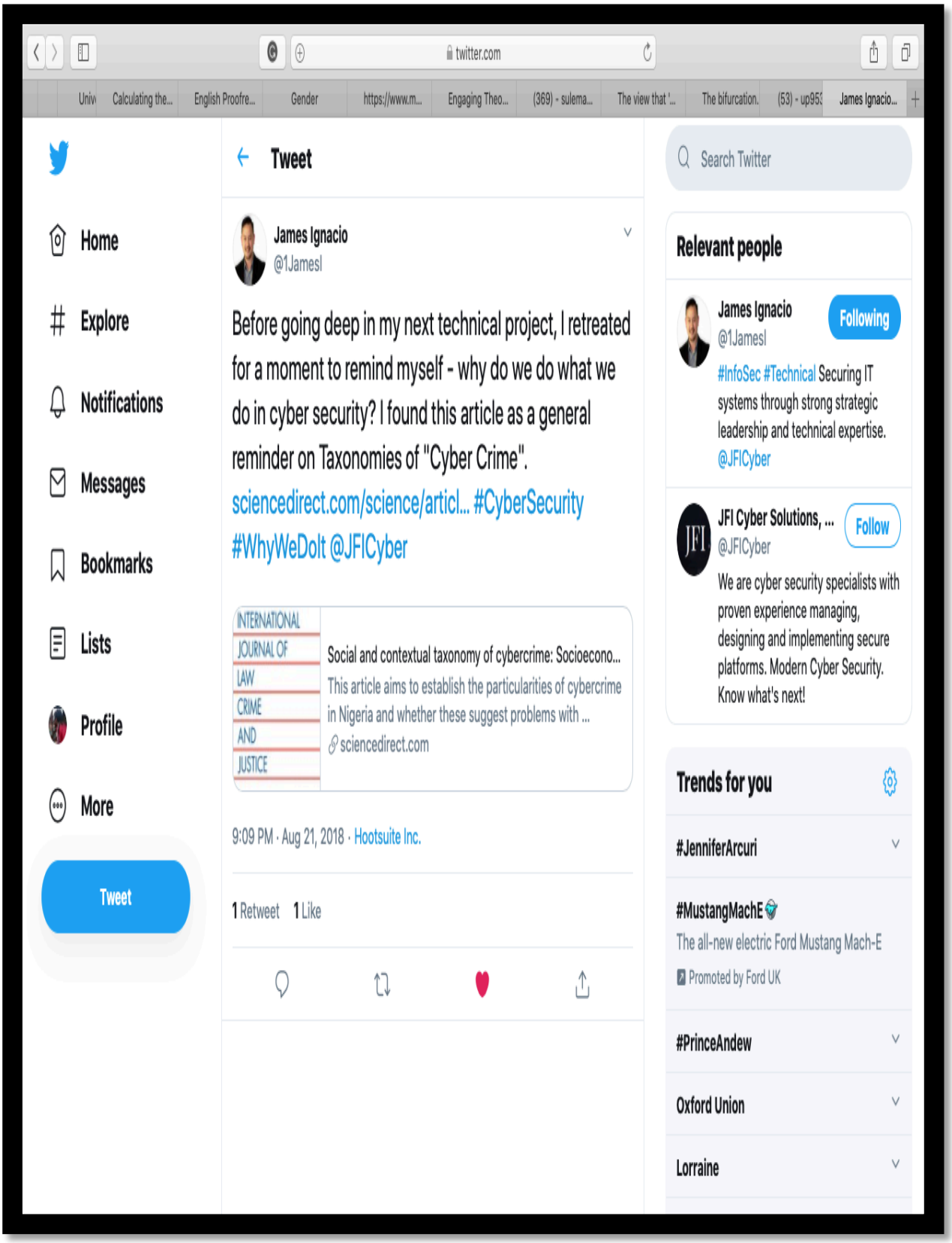
Appendix 10B



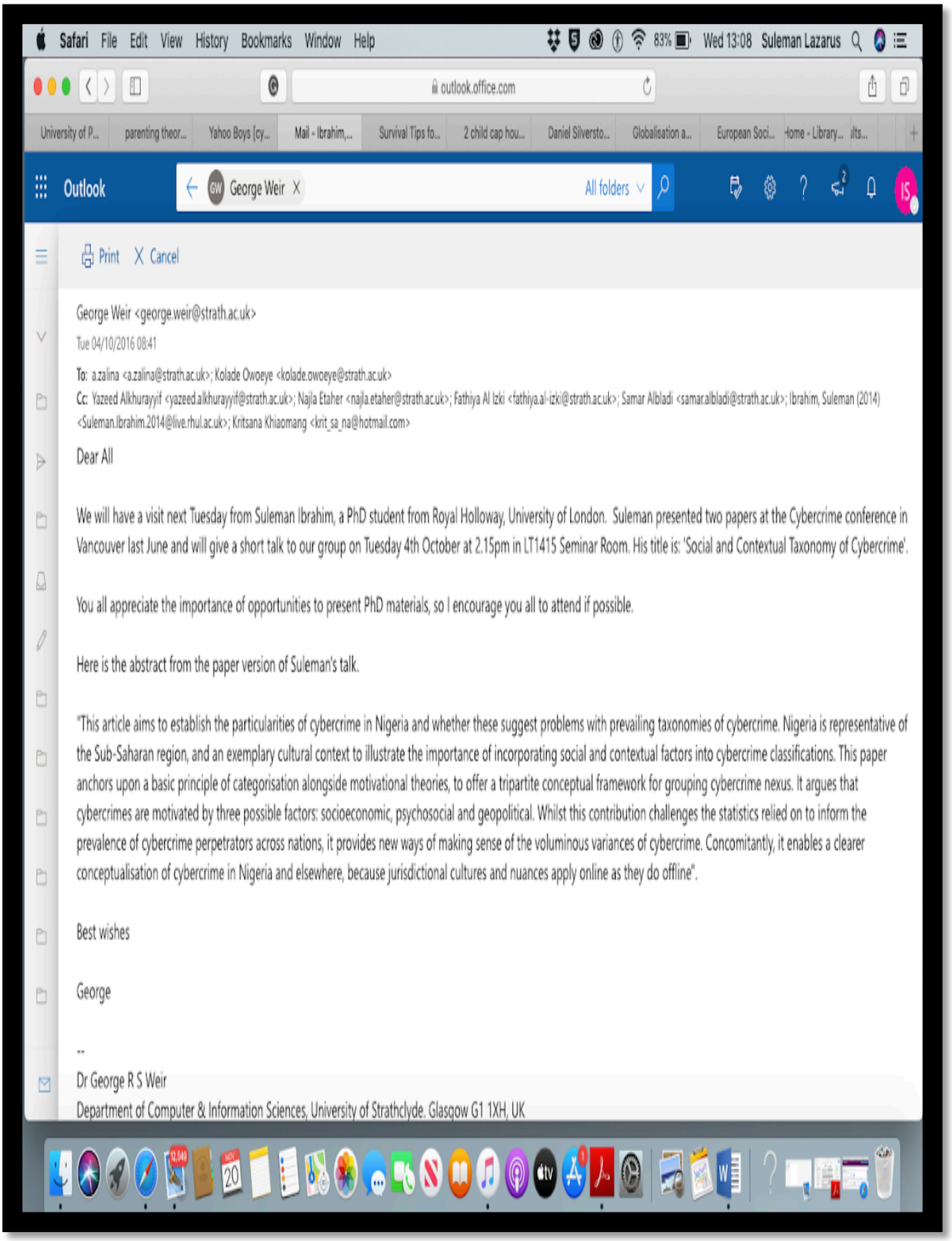
Appendix 11


Safari File Edit View History Bookmarks Window Help
73% Sun 1 Dec 13:36:36
theconversation.com
Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists | Published i...
The view that '419' makes Nigeria a global cybercrime player is misplaced
6 Comments
Oldest
Newest
Sign in to comment
Apeh Omede
Suleman Ibrahim, I totally agree with you and I think this is a better, enlightened and well-informed perspective about this subject. There's more to what cybercrime involves than just relegating it to cyberfraud only when it comes to Nigeria. Because of the way we are viewed globally as a result of such classification, I have seen advise like not including your nationality in your resume or CV as a Nigerian, so that the organisation doesn't judge you by that but by the quality of your works and let then find out themselves where you are from and decide what to do after that. I know many of us with good intentions and are doing great works all over the world, yet this kind of perspective does not help in any way. There is a sincere need to review this kind of categorization.
3 years ago • Report
Jon Richfield
connecté avec Facebook
Though I can well understand Apeh's dismay and resentment, which I should think would remain equally justifiable if every criticism of Nigeria as a country were valid, and it is equally easy to understand that the article author shares his feelings, because the unjustified generalisations reflect framing rather than a valid assessment of Nigerian criminality.
On the other hand, to argue that it follows that it is vital to point out that Nigerian hands should be ranked as no dirtier than some other countries', on the grounds
Read more
3 years ago • Report

Appendix 12


twitter.com
Tweet
James Ignacio
@1JamesI
Before going deep in my next technical project, I retreated for a moment to remind myself - why do we do what we do in cyber security? I found this article as a general reminder on Taxonomies of "Cyber Crime". sciencedirect.com/science/articl... #CyberSecurity #WhyWeDoIt @JFICyber
INTERNATIONAL JOURNAL OF LAW CRIME AND JUSTICE
Social and contextual taxonomy of cybercrime: Socioecono...
This article aims to establish the particularities of cybercrime in Nigeria and whether these suggest problems with ...
sciencedirect.com
9:09 PM · Aug 21, 2018 · Hootsuite Inc.
1 Retweet 1 Like
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
Search Twitter
Relevant people
James Ignacio
@1JamesI
Following
#InfoSec #Technical Securing IT systems through strong strategic leadership and technical expertise. @JFICyber
JFI Cyber Solutions, ...
@JFICyber
Follow
We are cyber security specialists with proven experience managing, designing and implementing secure platforms. Modern Cyber Security. Know what's next!
Trends for you
#JenniferArcuri
#MustangMachE
The all-new electric Ford Mustang Mach-E
Promoted by Ford UK
#PrinceAndew
Oxford Union
Lorraine

Appendix 13



Safari File Edit View History Bookmarks Window Help 83% Wed 13:08 Suleman Lazarus

outlook.office.com

University of P... | parenting theor... | Yahoo Boys [cy... | Mail - Ibrahim,... | Survival Tips fo... | 2 child cap hou... | Daniel Silversto... | Globalisation a... | European Soci... | Home - Library... | ilts...

Outlook | George Weir X | All folders

Print | Cancel

George Weir <george.weir@strath.ac.uk>

Tue 04/10/2016 08:41

To: a.zalina <a.zalina@strath.ac.uk>; Kolade Owoeye <kolade.owoeye@strath.ac.uk>

Cc: Yazeed Alkhurayyif <yazeed.alkhurayyif@strath.ac.uk>; Najla Etaher <najla.etaher@strath.ac.uk>; Fathiya Al Izki <fathiya.al-izki@strath.ac.uk>; Samar Albladi <samar.albladi@strath.ac.uk>; Ibrahim, Suleman (2014) <Suleman.Ibrahim.2014@live.rhul.ac.uk>; Kritsana Khiaomang <krit_sa_na@hotmail.com>

Dear All

We will have a visit next Tuesday from Suleman Ibrahim, a PhD student from Royal Holloway, University of London. Suleman presented two papers at the Cybercrime conference in Vancouver last June and will give a short talk to our group on Tuesday 4th October at 2.15pm in LT1415 Seminar Room. His title is: 'Social and Contextual Taxonomy of Cybercrime'.

You all appreciate the importance of opportunities to present PhD materials, so I encourage you all to attend if possible.

Here is the abstract from the paper version of Suleman's talk.

"This article aims to establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrime. Nigeria is representative of the Sub-Saharan region, and an exemplary cultural context to illustrate the importance of incorporating social and contextual factors into cybercrime classifications. This paper anchors upon a basic principle of categorisation alongside motivational theories, to offer a tripartite conceptual framework for grouping cybercrime nexus. It argues that cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical. Whilst this contribution challenges the statistics relied on to inform the prevalence of cybercrime perpetrators across nations, it provides new ways of making sense of the voluminous variances of cybercrime. Concomitantly, it enables a clearer conceptualisation of cybercrime in Nigeria and elsewhere, because jurisdictional cultures and nuances apply online as they do offline".

Best wishes

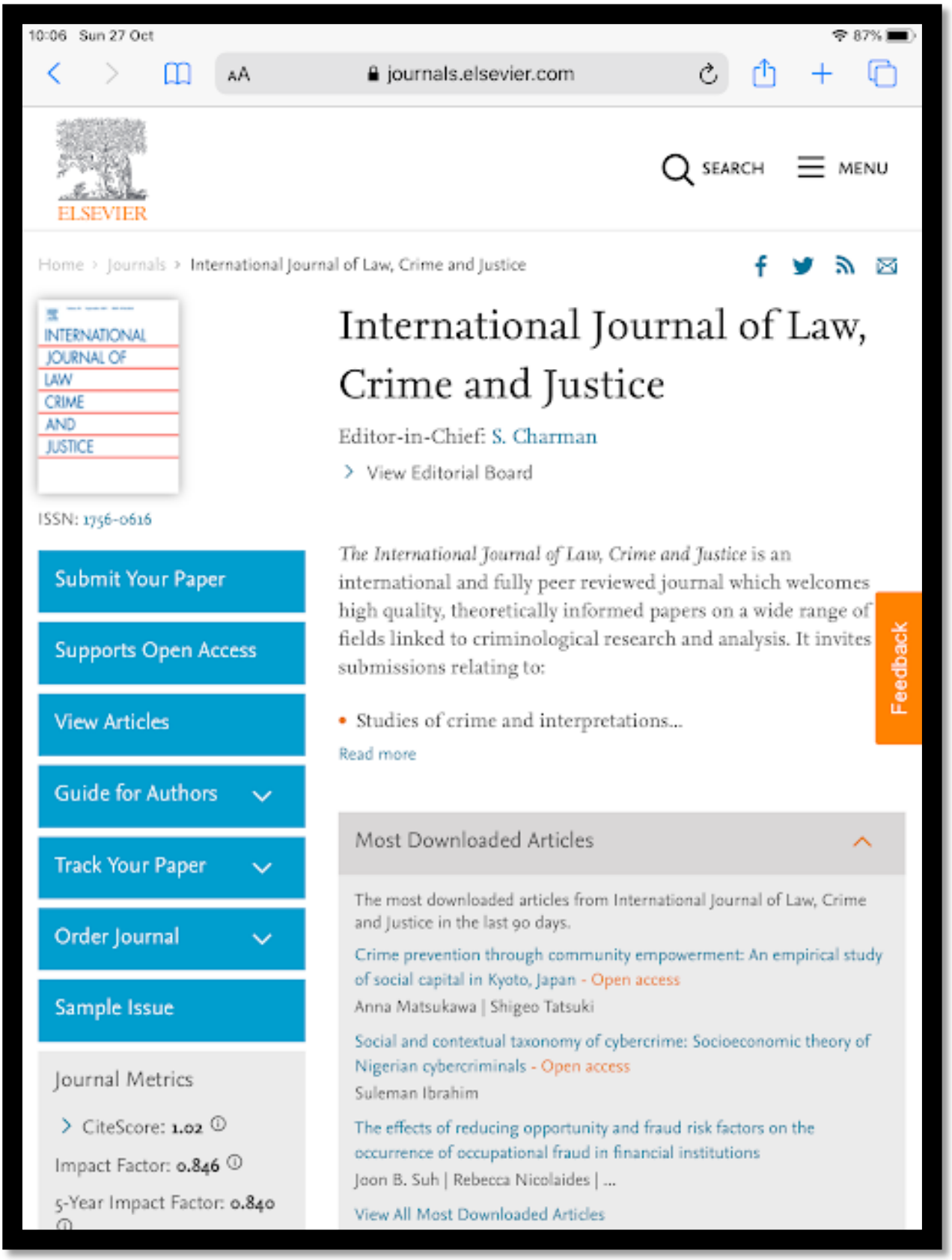
George

--

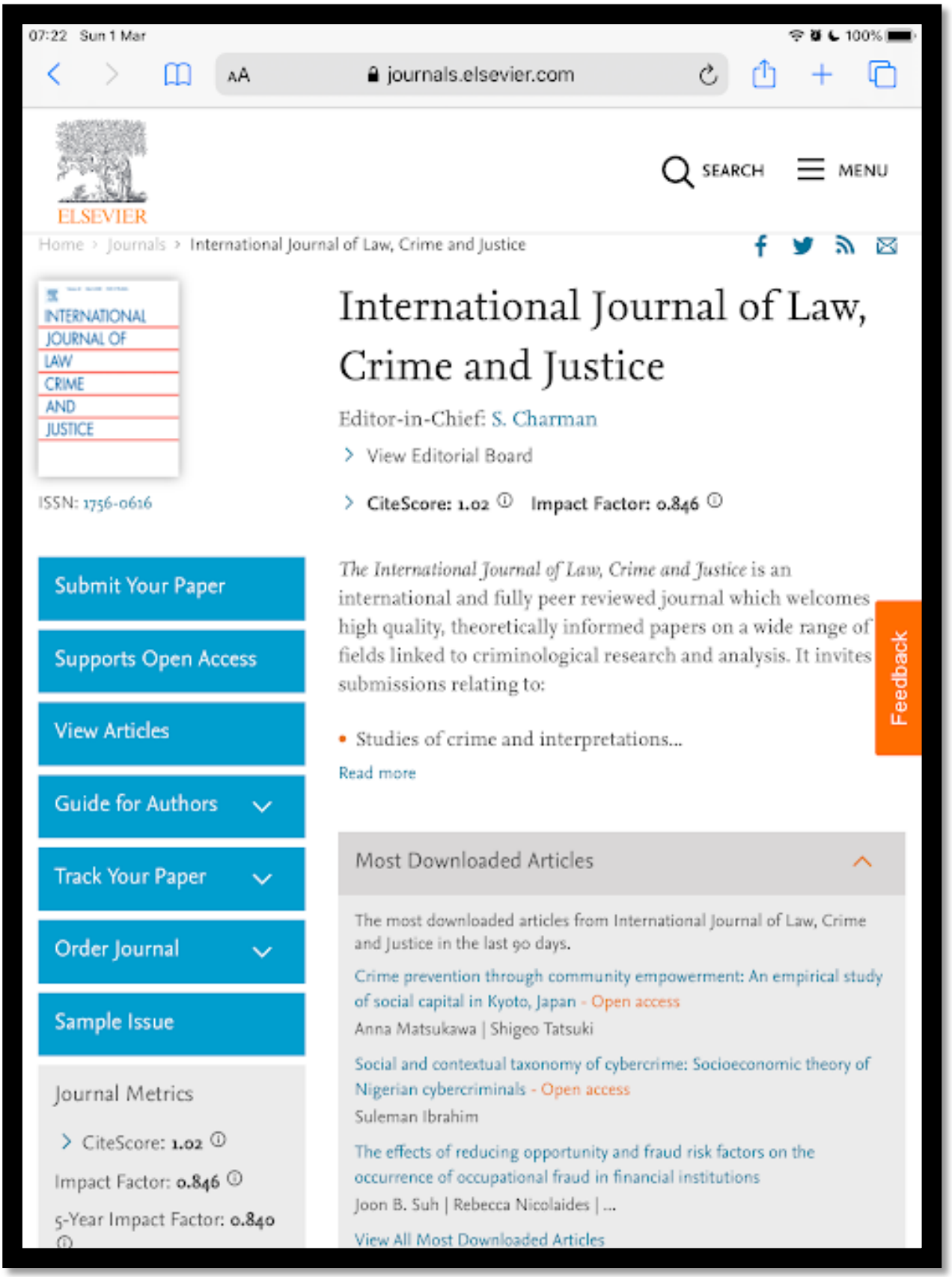
Dr George R S Weir

Department of Computer & Information Sciences, University of Strathclyde, Glasgow G1 1XH, UK

Appendix 14A



Appendix 14B



Establishing the Particularities of Cybercrime in Nigeria: Theoretical and Qualitative Treatments

By

Suleman Lazarus

PhD by Publication
Volume Two

University of Portsmouth
Institute of Criminal Justice Studies
March 2020

This commentary and publications are submitted in part fulfilment of the requirements of the University of Portsmouth for the degree of PhD by Publication

The list of six peer-reviewed publications included

• Ibrahim[8], Suleman. (2016a). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice,* 47, 44-57.
• Ibrahim, Suleman. (2016b). Causes of Socioeconomic Cybercrime in Nigeria. In IEEE *International Conference on Cybercrime and Computer Forensic* (ICCCF), Vancouver, BC, Canada (pp. 1-9). *IEEE* Publishing.
• Lazarus, Suleman. (2018). Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists. *Criminology, Criminal Justice, Law & Society*, 19, (2), 63-81.
• Lazarus, Suleman. (2019a). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, 10, (3), 146, 1-20.
• Lazarus, Suleman. (2019b). Just Married: The Synergy between Feminist Criminology and the Tripartite Cybercrime Framework Journal. *International Social Science Journal*, 69, (231), 15-33.
• Lazarus, Suleman, & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, 40, 14-26.

[8] In 2017, I changed my surname from Ibrahim (paternal) to Lazarus (maternal).

International Journal of Law, Crime and Justice 47 (2016) 44–57

Contents lists available at ScienceDirect

International Journal of Law, Crime and Justice

journal homepage: www.elsevier.com/locate/ijlcj

Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals

Suleman Ibrahim

The Center for Doctoral Training in Cyber Security, The Information Security Group, Royal Holloway University of London, TW20 0EX, Surrey, UK

ARTICLE INFO

Article history:
Received 16 May 2016
Received in revised form 12 July 2016
Accepted 19 July 2016
Available online 11 August 2016

Keywords:
Cybercrime taxonomy
Socioeconomic cybercrime
Nigerian 419 fraud
Cybercrime classifications
Definitions of cybercrime
Tripartite cybercrime framework

ABSTRACT

This article aims to establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrime. Nigeria is representative of the Sub-Saharan region, and an exemplary cultural context to illustrate the importance of incorporating social and contextual factors into cybercrime classifications. This paper anchors upon a basic principle of categorisation alongside motivational theories, to offer a tripartite conceptual framework for grouping cybercrime nexus. It argues that cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical. Whilst this contribution challenges the *statistics relied on to inform the prevalence of cybercrime perpetrators across nations, it* provides new ways of making sense of the voluminous variances of cybercrime. Concomitantly, it enables a clearer conceptualisation of cybercrime in Nigeria and elsewhere, because jurisdictional cultures and nuances apply online as they do offline.

© 2016 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

This paper sets out with the aim of developing and improving upon existing taxonomies used in cybercrime scholarship. Listed in prevalence of cybercrime perpetrators, Nigeria, the UK and the USA (in ascending order of significance) are on top of the 'league table' (Internet Crime Complaint Center - ICCC, 2006–2010). Considering Nigeria as an exemplary social context – representing the Sub-Saharan world region - this article will emphasise the need to incorporate social and contextual factors into the classification schemas. Whilst the establishing of the particularities of cybercrime in Nigeria will concomitantly suggest problems with prevailing taxonomies of cybercrime, it will also render problematic, the basis for ICCC's (2006–2010) claim on the prevalence of cybercrime perpetrators.

Whilst cybercrime primarily operates in the realm of cyberspace, terrestrial crimes operate in physical spaces (Manjikian, 2010). Seeking to summarise and encapsulate various conceptualisations within cybercrime literature, Yazdanifard et al. (2011) defined 'cybercrime' as 'any type of intentional criminal scheme that is computer or/and internet-mediated'. However, whilst such a description describes a wide spectrum of cybercrime, it fails to account for the dual model of criminal schemes within [1]cyberspace. Ogwezzy (2012, p.91) elaborated that the term 'cybercrime' implies "offences committed through the use of the computer in contrast to 'computer crime' which refers to offences against the computer and data or

E-mail address: suleman.ibrahim.2014@rhul.ac.uk.

[1] Cyberspace is a borderless global space, a site for the globalization of threats as well as benefits (Manjikian, 2010).

http://dx.doi.org/10.1016/j.ijlcj.2016.07.002
1756-0616/© 2016 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

program therein". Whilst the computer and its content are the primary targets in computer crimes, the meaning of cybercrime is wrapped around the use of a computer or/and the Internet to commit age-old crimes (Ogwezzy, 2012; McGuire and Dowling, 2013).

Conceptions of 'computer crime' and 'cybercrime' interpenetrate one another; their entities are intertwined and therefore difficult to disentangle. The intertwining of computer crime and cybercrime further challenges the simplistic rendering of cyberspace and physical space as two different entities with easily defined boundaries. Regarding 'cybercrime', there are over 30 types identified in existing literature, since cyberspace-crime linkage was first constructed in cyberpunk stories (Wall, 2008). Most of them are listed in Table 1 below. These numerous variances are implicated in obscuring the effective conceptualisation of 'cybercrime'. Yet, whilst the existing dichotomised categories (Gordon and Ford, 2006; McGuire and Dowling, 2013) adhere to the basic psychological principle of categorisation (Rosch, 1978), they fail to acknowledge the roles of motivations in offending. Relatedly, when the existing motivational categories (Chawki et al., 2015a; Wall, 2013) do consider the motivational element of offending, they take for granted the basic psychological principle of categorisation. Insights from Rosch's (1978, p.28) general and basic principles for the formation of categories stipulate that:

> "the task of category systems is to provide maximum information with the least cognitive effort [and] the perceived world comes as structured information rather than as arbitrary attributes. Thus maximum information with least cognitive effort is achieved if categories map the perceived world structure as closely as possible. This condition can be achieved either by the mapping of categories to given attribute structures or by the definition or redefinition of attributes to render a given set of categories appropriately structured".

In line with motivational theories framed within the basic psychological framework of categorisation, this current endeavour will, firstly, aim not only to complement the existing categories but also offer a more conceptually robust framework for grouping cybercrime. The implication being that whilst cybercrimes constitute a global problem, recognising the limits of a 'one size fits all' binary of taxonomies is of utmost importance. Secondly, Nigeria will be presented as an exemplary cultural context to illustrate certain aspects of these limitations (binary model) and the importance of social/contextual factors in the classification schemas. Through the precise delineation of the particularities of cybercrime in Nigeria, this article aims to determine the extent to which this exemplar problematises or contradicts prevailing taxonomies of cybercrime. At its core, this paper has three research questions, which it will aim to answer: firstly, how useful are the existing cybercrime taxonomies in making sense of social and contextual factors (such as the category of cybercrimes that the Nigerian cybercriminals exclusively commit)? Secondly, since 'cybercrime' is a globalised phenomenon, how is the Nigerian case - representing the Sub-Saharan region, any different from Western regions? Thirdly, what exactly is 'cybercrime' in a Nigerian context?

2. A dual model of cybercrime

The word 'cybercrime' comprises a wide range of online crimes. For McGuire and Dowling (2013, p.5), "[C]yber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other forms of ICT [Information and Communications Technology]" such as creation or/and distribution of malwares/viruses. On the other hand, cyber-enabled crimes "can still be committed without the use of ICT" such as cyber fraud. These dual categories are illustrated in Fig. 1. Unlike traditional crimes however, one criminal scheme in the realm of cyberspace may involve multiple nations and actors and even impact on multiple nations simultaneously (Yazdanifard et al., 2011). Thus whilst traditional crime tends to be regarded locally, cybercrime is usually considered on a global scale (Yar and Jewkes, 2010). For example, if a person in Russia creates computer 'viruses/malwares' while another person in Nigeria rents it to send credit scam e-mails and a third party in the USA transfers funds using the illegally acquired data, (Wall, 2013), all three individuals are implicated in different strands

Table 1
Tripartite cybercrime framework (TCF).

Socioeconomic cybercrime	Psychosocial cybercrime	Geopolitical cybercrime
*Hackers and crackers	*Hackers and crackers	*Hackers -'Hacktivist'
Cyber fraud	Child pornography	Cyber spies
Cyber embezzlement	Cyber stalking	Cyber espionage
Cyber piracy	Cyber bullying	***Cyber terrorism
Cyber blackmail	Revenge porn	Cyber Vandalism
Romance scam	Cyber rape	Cyber assault
Online drug trafficking	*Cyber hate speech	*Cyber hate speech
Cyber prostitution	*Cyber extortion	Cyber riot
*Cyber extortion	Obscenity	Cyber sabotage
Illegal online gambling	*Cyber-prostitution	Cyber-colonialism
*Cyber Trespass	*Cyber Trespass	Cyber rebellion
***Cyber terrorism	*Cyber homicide	
	***Cyber terrorism	

*Where the type of cybercrime appears in more than one column.
***Where the type of cybercrime appears in more than two columns.

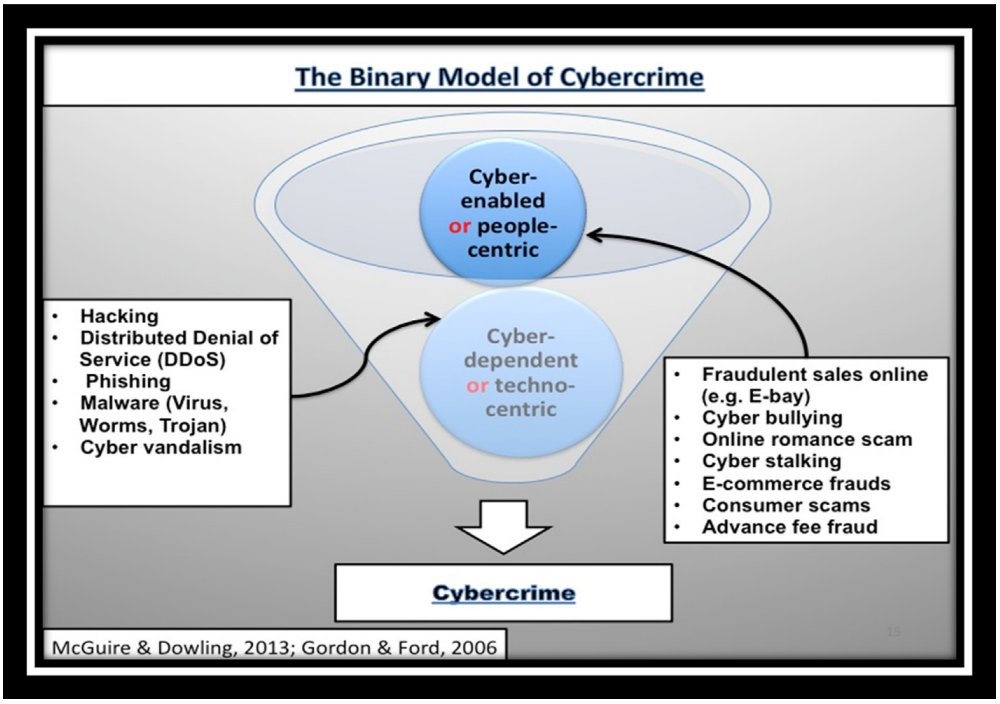


Fig. 1. The binary model of cybercrime.

of cybercrime. Whilst all three actors are motivated by monetary benefits, they are in fact involved in cyberspace in varying degrees. The virus/malware creator has committed a cyber-dependent offence, whereas the other two have committed cyber-enabled offences. This existing traffic between cyber-enabled and cyber-dependent categories clearly illustrates the complexity of cybercrime and how one criminal act can impact on multiple nations and involve various networks of actors simultaneously.

Closely related to cyber-enabled and cyber-dependent categories are 'techno-centric (type I) and people-centric (type II) subsets'. Gordon and Ford (2006, p.15) specifically posited that techno-centric and people-centric cybercrime are at the opposite ends of a continuum; dichotomising cybercrime based on the strength of the cyber-element versus people-component of the criminal act in question. They distinguished Type I (techno-centric) crimes such as e-commerce fraud, cyber-vandalism, data manipulations through hacking, phishing, from Type II (people-centric) crimes such as cyber fraud, cyber bullying and cyber-stalking as illustrated in Fig. 1. The latter being less technologically oriented than the former and therefore grounded in perpetrator-victim interactions. These binary models (people-centric and techno-centric; cyber-enabled and cyber-dependent), anchoring on a basic psychological principle of categorisation, have no doubt offered a useful tool in looking at voluminous cybercrime variances.

However, motivational elements are not configured in the properties of these binary typologies. As a result, they are ill-equipped to differentiate between the psychological-motivated cybercrimes such as cyber stalking and cyber bullying from financially motivated ones such as cyber fraud and cyber embezzlement. Simply put, they have taken for granted the motivational lens of looking at cybercrime, which renders them unable to answer a simple question: how exactly is a digital crime that is primarily geared towards defrauding a person or a group of persons, different to another online scheme intended to fundamentally disrupt a person's psychological state of mind? It is essential to isolate the primary motive behind cybercrimes in the meaning-making of what any particular cybercrime is in a given context, as illustrated in Table 2 below.

It is reasonable therefore to argue for grouping cybercrimes according to criminals' motivations. This could and would sharpen the distinction between cybercrimes that are rooted in financial gains such as cyber fraud, and psychologically motivated cybercrimes such as cyber stalking. However, conceptually, the above binary models appear to be 'explanatory-tools', which cannot capture the differences between cybercrimes primarily driven by financial rewards and cybercrimes fundamentally propelled by psychological benefits as shown in Table 2. Based on these rationales, it is reasonable to complement these models - 'techno-centric and people-centric (Gordon and Ford, 2006) and cyber-enabled crime and cyber-dependent (McGuire and Dowling, 2013). That said, the existing motivational categories, despite usefulness in acknowledging the motivational element of cybercrime, have their limitations too.

3. Some existing motivational taxonomies

In endorsing motivational categories, Chawki et al. (2015a, p.16–17) argued that it is crucial to understand a person's profile in the case of a particular cybercrime. Particular educational attainment, occupation and childhood experiences, he

Table 2
Perpetrators' benefits and victims' losses.

Attacker/attacked	Socioeconomic	Psychosocial	Geopolitical
Perpetrator (primary benefits)	Economic gain	Psychological gain	Geopolitical, economic & psychological losses
Victim (primary loss)	Economic loss	Psychological distress	Geopolitical, economic & psychological losses
Perpetrators (secondary benefits)	Both economic & psychological gains	Psychological gain	Geopolitical, economic & psychological gains
Victim (secondary loss)	Both economic & psychological losses	Both economic & psychological losses	Geopolitical, economic & psychological losses

argued, help shed light on the individual implicated in any cybercrime. As Chawki et al. (2015a) further postulated that cybercriminals can be categorized as: [a] children and adolescents [b] organized hackers [c] professional hackers [d] discontent employees. Whilst Chawki et al.'s (2015a) categories tell us about different levels of sophistication involved in offending (e.g., professional hackers and organized hackers), they also reveal the extent to which cybercriminals could be age-graded.

However, cross-cultural insights from young offenders have pointed out that age is not lived similarly across cultures and age-related behaviours are constituted differently across cultures (Brathwaite, 1996; Cain, 2000). For example, in line with Tade and Aliyu's (2011) sociological work in Nigeria and Armstrong's (2011) anthropological analysis in Ghana, most 'young people' in Nigerian and Ghanaian universities *involved in cybercrime in general* are involved in cyber fraud *in particular*. In contrast, studies on Canadian undergraduates (Cunningham et al., 2014; Faucher et al., 2014) university students in the USA (Lindsay and Krysik, 2012) 'young people' in Finland (Oksanen and Keipi, 2013) and higher education students in Britain (Benson et al., 2015; Boulton et al., 2012) suggest that young people in Canada, Finland, the USA, and Britain – the Western world region, are more involved in psychological-oriented cybercrime such as cyber bullying and cyber harassment than cyber-fraud. The key point is that "young people" as a category is insensitive to the differentiation between 'what is true of all societies' and 'what is true of one society at one point in time and space' (Nelken, 2010). Another limitation is that, Chawki et al.'s (2015a) taxonomy does not adhere to the basic principles of categorisation.

In a similar vein, Wall 2007 (2013, p.62–65) proposed seven different motivational subsets, based on: self-satisfaction; the need for peer respect; to impress potential employers; criminal gain or commercial advantage; revenge; distance from victim; politically motivated protest. These motivational signposts help to illustrate that the specific motivations behind cybercrime are diverse. An equally important issue is that the seven subsets for cyber offenders, as revealed by their titles, shed more light on the drives, the 'push and pull factors' of cybercriminals to cybercrime (Wall, 2013). The value of this grouping is most evident in the 'criminal gain or commercial advantage', and 'politically motivated' categories. For example, whilst some types of cybercrime such as cyber extortion, cyber fraud and cyber embezzlement fit squarely under the canopy of the former, cyber espionage, cyber terrorism, cyber rebellion, can be located smoothly in the sphere of the latter.

There is however, a primary limitation of this taxonomy, as aforementioned, in that it neglects the basic principle of categorisation. Some of the proposed groups, such as 'distance from the victim', involve almost all types of cybercrime. Indeed, 'distance from the victim' is a specific aspect of most cybercrimes as Brown (2001) intimated in the analysis of cost-benefits and economics of criminal conducts. Similarly, 'self-satisfaction' - rooted in the utilitarian maximisation principle - may be in the form of tangible things such as monetary reward or intangible ones such as psychological thrill. Either way, 'self-satisfaction' is integral to almost all types of cybercrime, and arguably does not seem to represent a specific category of cybercrimes.

In the same vein, 'revenge' as a category could be the driver of cyber stalking, cyber fraud, or hacking. Whilst 'revenge' may be a principal impetus behind this range of cybercrimes, it requires a lot of cognitive effort to see the 'rope' that binds them together as a distinct subset. *'Thus maximum information with least cognitive effort is only achievable if categories map the perceived world structure as closely as possible'* (Rosch, 1978, p.28). The crux is that existing motivational categories (Chawki et al., 2015a; Wall, 2013) have ignored a basic psychological principle of categorisation (Rosch, 1978, p.28): 'to simplify a complex set of data and increase information intake with the least cognitive effort'.

4. The tripartite cybercrime framework (TCF)

In complementing the above taxonomies, this current endeavour anchors on the basic psychological principles of categorisation alongside motivational insights to offer a [2]*tripartite-cybercrime-framework* (TCF). An individual is said to be motivated when such an individual is moved, energised, or inspired to do something (Deci and Ryan, 2011, 2000, 1985). Motivation is orientation graded; it varies according to the underlying variable behind the actions in question. It can also vary in terms of the intensity of occurrence, i.e., whether a person is highly motivated or otherwise. Whilst the latter centers on the amount or size of impetus behind the action, the former is concerned with the reason for the action. Arguably motivation can be conceptualised as the foundation of most crimes; it is reasonable therefore to offer a social/contextual basis for the

[2] This article uses the tripartite cybercrime framework (TCF) or the tripartite conceptual framework (TCF) interchangeably.

categorizing of cybercrime. Self-Determination Theory (Deci and Ryan, 2011; 1985) specifically argues that motivational types - intrinsic and extrinsic, define the strength or intensity of motivation.

Motivation therefore can be schematised as a dual phenomenon; incorporating intrinsic and extrinsic motivations. This binary model is necessary for the precision of illustrations and the discussion that follows. Whilst extrinsic motivation is the doing of an activity solely to achieve a distinct result, intrinsic motivation is the demonstration of actions inherently for the mere satisfaction of doing them (Deci and Ryan, 2011; 1985). For example, a poet is more likely to write poems for the inherent satisfaction of such an activity rather than for the approval of his/her parents – intrinsic motivation; whereas a student is more likely to study hard for good grades and a better future – extrinsic motivation. The majority of activities are generally propelled by extrinsic motivation, i.e., people fundamentally motivated to do something due to the direct and expected consequence of their actions (Deci and Ryan, 2011; 1985).

However, as Kshetri (2006), in describing cybercriminals – hackers – emphasised, intrinsic motivation may have a superior impact compared to extrinsic motivation. This paper conceptualises extrinsic and intrinsic motivations of cyber crimes as twin interlocking entities, which are difficult to disentangle, and, as Wehmeyer and Little (2009) note, extrinsically motivated behaviours can parallel intrinsically motivated activities if actors internalise their actions, and experience flow in their activities. Nevertheless, Layous et al. (2013) pointed out that intrinsically motivated people are more likely to experience flow than those who are extrinsically motivated. Nakamura and Csikszentmihalyi (2002, p.95) defined flow as "the balance of challenges and skills when both are above average levels for the individual". This suggests that it is a state of profound task-absorption and task-enjoyment experience, most likely to condition the actor involved to lose sense of time in doing the task in question (Csikszentmihalyi, 1990, 2000, 2014). Flow experience has the following nine components: [a] Clarity of goals at every stage [b] Availability of immediate feedback [c] a balance between challenges and skills [d] Interpenetrations of action and awareness [e] Limited distractions from consciousness [f] Absence of concern in terms of failure [g] The disappearance of self-consciousness [h] The distortion of sense of time [i] The activity is autotelic (Csikszentmihalyi, 1990, 2000, 2014). Arguably, flow experience is crucial to the understanding of cybercrime motivations.

Given that the type of primary motivation behind an action matters in relation to the opposing forces that could inhibit the intended action, underlines the importance of incorporating social factors into classification schemas. This paper also acknowledges that certain types of cybercrimes listed in Table 1 fit into two or more motivational categories. Although there are some degrees of overlap between the categories, the primary motivation behind the action is the basic tool to differentiate between types of cybercrimes. For example, whilst cyber fraud is under the socioeconomic cybercrime category, revenge porn is under the umbrella of psychosocial cybercrime, as illustrated in Table 1. Theoretically therefore, in complementing the existing categories, this paper provides a more refined motivational taxonomy based on perpetrators' primary benefits as well as victims' primary loss, as shown in Table 2.

As Tables 1 and 2 fundamentally illustrate, in socioeconomic cybercrimes, the perpetrator often has a direct contact with his/her victim; this can be defined as financially motivated crimes that are computer or/and internet-mediated, such as online fraud, romance scam, and e-embezzlement. Psychosocial cybercrime are cybercrimes, which are principally psychologically driven such as cyber stalking, cyber harassment and cyber rape. Whilst socioeconomic cyber criminals may aim to deflate the economy of their victims, psychosocial cyber criminals focus fundamentally on inflicting psychological distress (full analysis of the implications of the TCF, can be found further down).

Yet there remains a considerable amount of similarity between the two loose categories. Unlike the viewpoint that not all actors are economically motivated (Hayward, 2007), the analysis of the motivational drives and economic decision-making in relation to crime in general is more refined (Farrell, 2010). According to Farrell (2010), the application of utility maximisation rather than monetary benefit or economic maximisation is a more appropriate term to deploy in conceptualising the general costs and benefits of crime. Hence, psychological benefits, including expressive emotional elements and sensations, are critical in determining if crime is economically motivated or not. Flowing from the above, different primary motivations underpin different types of cybercrimes identified in literature – listed in Table 1. Collaterally, victims of cybercrimes may suffer differently based on the primary motivation - the perpetrators of cybercrime in question as shown in Table 2. Therefore, this current paper proposes that cybercrimes are motivated in three different ways: socioeconomic, psychosocial and geopolitical.

In terms of the penetrator-victim transactions, the primary driving forces behind cyber bullying, online harassment and cyber stalking are psychological in nature. Unlike fraud-based cybercrimes, the injuries as well as the benefits lie within the realm of the mind. The above distinction is not to suggest that acquisitive motivations involved in financial crimes are absolutely non-psychological. Insights from health psychology (Lazarus, 2006; Lazarus and Folkman, 1984a, 1984b) support the fact that financial loss (e.g. due to cyber fraud) can manifest physiologically as distress. However, the key element of differentiation between socioeconomic and psychosocial categories is that the primary benefits of the perpetrators as well as the primary losses of victims are different, as illustrated in Table 2. In contrast, under the binary model discussed above, both socioeconomic and psychosocial cybercrimes are grouped as one, that is, cyber-enabled crimes. Whereas the lens of the TCF can further differentiate between the two, as well as a third category: geopolitical (as discussed further below).

For example, when these [3]cybercriminals deploy the '*Freestyle trick*' using accounts on dating sites to befriend/condition unsuspecting victims to the point that they 'fall in love' with them and support them financially, the victims of Nigerian

[3] The '*Freestyle trick*' is a preferred/common method of operation among the early career cybercriminals in Nigeria, possibly because it is the simplest one among multitude of others.

cybercriminals' '*Freestyle trick*', may suffer psychological distress as well as financial loss, but the primary aim of the perpetrators is commercial gain. In terms of the predicament of victims, economic losses are more grounded in the quantifiable realm than psychosocial cybercrimes that are in the sphere of the mind.

On the other hand, geopolitical cybercrimes can be defined as those e-crimes that involve agents of statecraft or/and industrial representatives (e.g. cyber espionage). Yet even geopolitical cybercrimes constitute some elements of socioeconomic and psychological cybercrimes as illustrated in Table 2. For example, Hacktivists, primarily aiming to make a political statement could expose sensitive data from the law enforcement agencies and their actions could have economic, psychosocial and geopolitical consequences on a person or group of people. The collective consequences of the tripartite categories could lead to a security fault, which this paper calls 'cyber insecurity', defined as a situation where security mechanisms in both the existing cyberspace and physical space cannot guarantee perfect security, nor have the full capacity to resist and respond to both intentional and unintentional cyberspace threats and hazards. In terms of victim-perpetrator interaction, while socioeconomic and psychosocial cybercrimes are fundamentally engineered and executed on individual levels, geopolitical cybercrimes, broadly speaking, are actions of state agents, groups of individuals against other groups, nations or industrial entities acting on behalf of more complex statecraft or vested interests. In other words, each group – especially but not limited to, socioeconomic and psychosocial cybercrimes - may involve individual actors or group actors as both targets and perpetrators. A crucial element of these categories – as illustrated in Table 2, is their capacity to simplify complex sets of information, given that there are over 30 types of cybercrimes identified in the existing literature. The TCF also help to enhance our understanding of 'cybercriminals', and their geopolitical, socioeconomic and psychosocial factors. Another significant issue is that, unless they go against the grain that constitutes 'normality' in their home country, agents of statecraft that commit geopolitical cybercrimes are rarely considered 'criminals' at all. The assumption underpinning this is that they represent authority, rather than subversion. Therefore it is the nation they represent that is categorized as criminal, unlike individual subcultural rule breakers such as the Nigerian [4]419 cybercriminals.

5. What is 'cybercrime' in Nigeria?

Drawing on the TCF as shown in Tables 1 and 2, the focus of this discourse confines itself to an examination of Nigeria – representing the Sub-Saharan region, as an exemplary cultural context. It is critical therefore to underscore the peculiar economic-benefit induced trend of cybercrime in Nigeria - generalisable to other Sub-Saharan nations such as [5]Ghana, which may not represent squarely the hydra-headed nature of cybercrime in Western societies. Although there are multiple variations on how '419 fraud' happens (e.g. Adogame, 2007; Igwe, 2007; Aransiola and Asindemade, 2011; FBI, 2016), monetary benefit is central to the Nigerian 419 fraud as illustrated in Fig. 2 (for fuller accounts on how 419 happens, see the above authors). Although cybercrime is a global phenomenon, in most Western nations, in addition to socioeconomic cybercrime, the term cybercrime represents a range of computer/Internet-mediated crimes under the umbrella of psychosocial and geopolitical cybercrimes – see Tables 1 and 2. Couched within the aim of establishing the particularities of cybercrime in Nigeria is a wider critique of prevailing taxonomies of cybercrime. Nigerian cybercriminals to date, have been consistently implicated in money-oriented rather than psychosocial and geopolitical cybercrimes. In fact, the convergence of emerging evidence reinforces that perpetrators of cybercrimes in Nigeria focus exclusively on cyber-fraud (Ojedokun and Eraye, 2012; Smith, 2008; Tade and Aliyu, 2011; Adogame, 2007; Doyon-Martin, 2015; Chawki et al., 2015b; Akpome, 2015; Ellis, 2016; Ibrahim, 2016). Arguably, the Nigerian 419 fraud invented and revolutionalised by Nigerian kingpins such as Fred Ajudua (Longe et al., 2010) is rooted in socioeconomics.

Given the foregoing remarks, cybercrime in Nigeria can be conceptualised simply as the use of computer/Internet to commit fraud. According to the yardstick of the binary model, the use of computer/Internet to commit fraud falls under the scaffolding of cyber-enabled crime (see Fig. 1). Unlike ICCC's (2010) survey, which concentrated mainly on a range of [6]cyber-enabled crimes as shown in Table 3, some recent enquiries which focused exclusively on cyber-dependent crimes could not locate Nigeria at the upper part of the cybercrime perpetrators' hierarchy (e.g. Kaspersky, 2016). This comparison between these observations support the notion that Nigerian cybercriminals are more implicated in cyber-enabled than cyber-dependent (or techno-centric cybercrime) listed in Fig. 1. Does this not suggest problems with prevailing taxonomies of cybercrime?

If we look at the Nigerian case through the lens of the binary model (see Fig. 1), the problem is that we would be led to conclude that cybercrime in Nigeria is just cyber-enabled. Cybercrime in Nigeria is fundamentally rooted in socioeconomics, whereas the cyber-enabled crime framework encompasses a range of other crimes such cyber-bullying and cyber rape. This is problematic. In terms of cyber-bullying and cyber rape, the perpetrators' gains and the victims' losses, as illustrated in Table 2, are primarily psychosocial unlike cyber-fraud (which is primarily rooted in economic gains/losses). It suggests problems with

[4] "419 is coined from section 419 of the Nigerian criminal code (part of Chapter 38: Obtaining Property by false pretences; Cheating) dealing with fraud. Nowadays, the axiom '419' generally refers to a complex list of offences which in ordinary parlance are related to stealing, cheating, falsification, impersonation, counterfeiting, forgery and fraudulent representation of facts" (Chawki et al., 2015b, pp.129).

[5] 'Nigeria and Ghana are Anglophone Sub-Saharan nations separated and surrounded by Francophone nations. Despite multiple ethnic variations within and across these two countries, they have similarities: British colonisation, English language, relatively, similar time of independence' (Ibrahim, 2015, p. 312).

[6] Cyber-enabled crime and people-centric cybercrime will henceforth be interchangeably used.

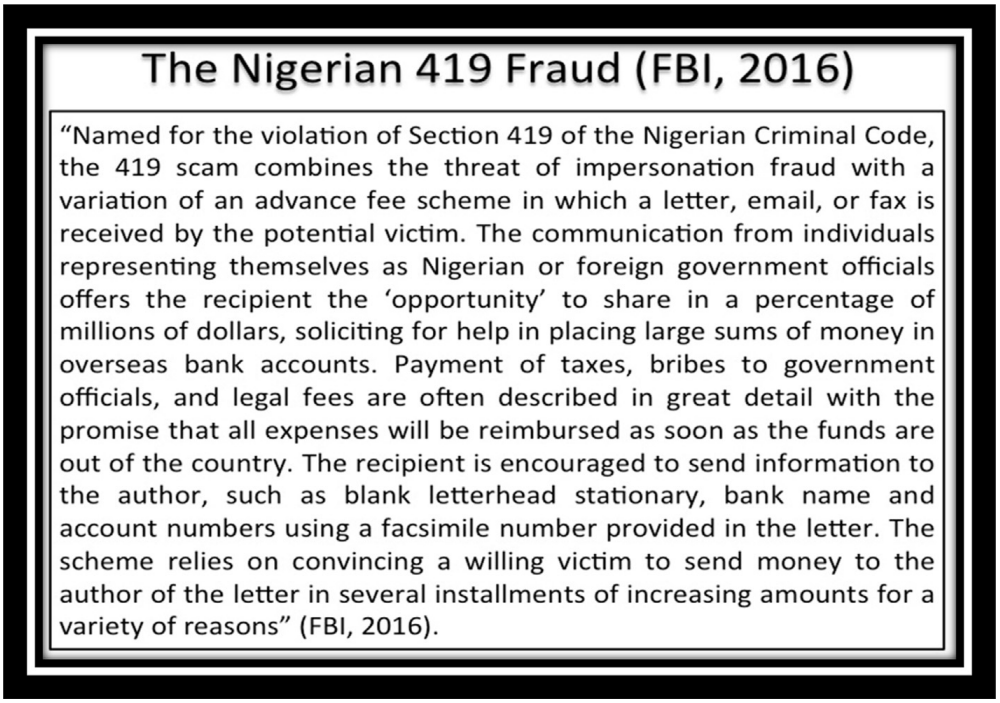


Fig. 2. How the Nigerian 419 happens.

Table 3
Top ten types of cybercrime covered by ICCC (2010).

Type	Percentage	Definitions
1. Non-delivery Merchandise	21.1%	Purchaser did not receive items purchased, or seller did not receive payment for items
2. FBI-Related Scams	16.6%	Scams in which a criminal poses as the FBI to defraud victims
3. Identity Theft	10.1%	Unauthorised use of victim's personally identifying information to commit fraud
4. Computer Crimes	9.3%	1) Crimes that target computer networks or devices directly 2) Crimes facilitated by computer networks or devices
5. Miscellaneous Fraud	7.7%	Variety of scams meant to defraud the public such as work-at-home scams and fraudulent contests
6. Advance Fee Fraud	6.1%	Criminals convince victims to pay a fee to receive something of value, but do not deliver anything of value to the victim
7. Spam	4.1%	Mass-produced, unsolicited bulk messages
8. Auction	4.0%	Fraudulent transactions that occur in the context of an online auction
9. Credit Card Fraud	3.6%	Fraudulent, unauthorised charging of goods and services to a victim's credit card
10. Overpayment Fraud	3.4%	An incident in which the complainant receives an invalid monetary instrument with instructions to deposit it in a bank account and send the deposited money back to the sender

the binary model because these other crimes under the umbrella of psychosocial cybercrime may not be primarily rooted in economic gains/loss (as illustrated in Table 2). In other words, whilst socioeconomic cybercrime constitutes only a sub-category of cyber-enabled crime, a cyber-enabled conceptual framework comprises a range of crimes other than cyber-fraud. Therefore, clearly, the existing binary categories discussed above are ill equipped to differentiate between psychosocial, socioeconomic and geopolitical cybercrime. The crux is that the evidence that support the centrality of socioeconomic cybercrime in Nigeria, concomitantly suggest problems with the dual model of cybercrime. These illustrations highlight the usefulness or utility of the TCF, which is more robust than the prevailing taxonomies in dealing with the complexities of numerous varieties of cybercrime.

6. Internet crime complaint centre: the critique of evidence

Having offered a theoretical critique of the prevailing models of cybercrime, this article will render problematic the basis for [7]ICCC's (2006–2010) claim on 'cybercrime perpetrators' league table', i.e., Nigeria being the third worst nation in the world. The FBI in partnership with the National White Collar Crime Center, aiming to reduce the volume of economic loss by

[7] It is noteworthy that unlike ICCC's (2006–2010), ICCC (2011–2014) reports exclude the perpetrators' league table.

Internet crime, established the Internet Crime Complaint Centre (ICCC or IC3) in May 2000. As its name implies, the ICCC is a center to receive victims' complaints concerning 'cybercrime' and over the past years, the ICCC received about 300,000 responses annually (ICCC, 2008; ICCC, 2009; ICCC, 2010; ICCC, 2011; ICCC, 2012; ICCC, 2013; ICCC, 2014; FBI, 2015). These data appear to be robust because they come directly from the people who experience the offence. However, the accuracy of responses were only self-reportedly measured, which highlights the ICCC's over-reliance on participants' honesty and accuracy. Secondly, given that it is only a small percentage of people who voluntarily report themselves as victims of cybercrime (Bohme and Moore, 2012) or crime in general (Reiner, 2010), the generalisability of the populist claim is questionable. In fact, according to the FBI (2014), less than 10% of people report themselves as victims of cybercrime globally. Apart from cybercrime being underreported, the vast bulk of cybercrime as Brenner (2007) and Brenner (2012) pointed out, is undetected. Arguably, even if an average of 300,000 respondents could be seen as a huge sample size in itself, it is far from being representative of the general population of all victims of cybercrime on earth. Additionally, there is the possibility that a majority of responses obtained by the ICCC may represent a selective group. For example, people who perceive themselves as 'victims' of the law are unlikely to channel their predicaments to the FBI. Also, Asian and African populations in the ICCC's global research were not significantly represented in comparison to North American and European populations. As Stevens (2011, p.9) reminded us, "statistics, even when they represent the underlying reality, are socially and selectively constructed, and cannot (or should not) simply speak for themselves". Therefore, regarding the cases that come to light, even if their statistical basis should be taken at face value, the claim is far from straightforward. A league table therefore is a pictorial representation of that construction, which not only renders invisible the process of construction, but also obscures the entirety of what it represents.

Thirdly, whilst the media and the political discourses tend to amplify the moral panic on the Nigerian 419 fraud (e.g. Adogame, 2007), Akpome (2015), in 'unsettling the myth of Nigerian exceptionalism' contended, there is an impossibility of knowing if every cyber-criminal using the Nigerian 419 letter/email templates is actually a [8]Nigerian citizen. It is reasonable also to point out that, there is an impossibility of knowing if some of those perpetrators grouped as 'Americans' or 'British' are not citizens of other nations. The key point here is that it is challenging to isolate cybercriminals from other nations and world regions who may have as Adogame (2007, p.7) pointed out, 'masked themselves as Nigerians and entered the theatre of 419 fraud as actors'. One of the implications is that, as Reiner (2010) noted, most people depend on the media, law enforcement agencies and politicians for 'authentic' information on issues such as crime. Regarding the Nigerian case, bearing in mind that some victims may not have accurate information about the actual perpetrators' identities, suggests that the media and political rhetoric on the 'Nigerian' fraud letter/emails may have unintended knock-on-effects on some victims reporting cybercriminals disproportionately as Nigerians. Given that 'there is a long-standing demonisation of Nigeria in the West as being full of criminals' (Agozino, 2003, p. 231) reinforces the notion that the ICCC's league table framed with a loose term 'cybercrime perpetrators' may have factored and impacted on some victims' perceptions.

Lastly, as shown in Table 3, over 90% of crimes covered (2006–2010) were primarily 'cyber-fraud' and under this specific category (which this article called socioeconomic cybercrime), Nigeria was found to be the third worst nation. Could the outcome be any different if geopolitical and psychosocial categories were covered? Given the limitations of the binary model, could the effect of the ICCC's report on various discourses be any different if the exclusion of geopolitical and psychosocial categories were made explicitly? This highlights the usefulness of the tripartite framework as it helps to simplify such league-table-claim into a nuanced umbrella (e.g. socioeconomic cybercrime). Unlike the popular representation of the ICCC's report in various discourses such as the media (e.g. 'Nigeria ranked third in the world for cybercrime' in Balancing Act, 2014), if we should view ICCC's (2006–2010) reports through the lens of the TCF, we could interpret it differently: 'cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical. As regards to the socioeconomic category, Nigeria was found to rank third in the world'. The term 'cybercrime' embodies multiple strands of crimes other than the socioeconomic category.

7. Further justifications for the usefulness of the TCF

In turn, this paper has developed another scope for categorizing cybercrime (TCF), having critiqued the prevailing taxonomies and rendered problematic the statistics relied on to inform the prevalence of cybercrime perpetrators across nations. Accordingly, it will henceforth offer further justifications for the usefulness of the TCF. One of the implications is that if the ICCC's reports and the likes are framed with TCF, the outcomes could be most precise. Concurrently, both the immediate outcomes and their subsequent knock-on-effects could be different and to a great extent, less ambiguous.

Let us suppose, hypothetically, that river A, B and C have between them the greatest numbers of 'animals' (fishes and reptiles) in the world: river A has 4000 fishes, and 2000 reptiles, river B has 2000 fishes and 8000 reptiles, river C has 3000 fishes and 6000 reptiles. If we were required to count the numbers of all the 'animals' in them and reported only our findings about fish, without applying the basic categorisation of 'animals' already in place, which includes reptiles as well as fish, we could and would be led to say that: 'regarding animals that live only in water, river A has 2000 more animals than river B and 1000 animals more than river C'. By the same token, river A, river C and river B – in descending order of significance, have the

[8] For example, the first known exponent of the present day 419 fraud, a former employee of Marine Department of the colonial government of Lagos in 1920 – 'Professor' Crentsil, came from Ghana (Ellis, 2016).

greatest numbers of animals that live only in water. We would then be led to conclude that river A has the greatest number of animals in the world when it is only in 'fish' category that river A is dominant. River B and river C both have more animals than river A in terms of the other category of animals called 'reptiles'. In fact, regarding the overall population of animals in these three rivers, in an ascending order of rank, river A, C, and B have the greatest number of animals in the world. This information is made easy because categories map the perceived world structure closely. The TCF could help to showcase data in a clear light by funneling information into nuanced umbrellas.

Beyond abstraction, TCF could be useful in policy-making processes, given that to simplify a complex set of data and maximise information intake with the least mental effort are at the heart of the TCF. The utilitarian value of the TCF could translate into policy-making processes because the instruments of persuasion in policy-making arenas, are often constructed with 'killer-charts' rather than elaborate text and analysis. 'Many policy documents transmitted between policy making civil servants are mostly characterised by bullet points and simple diagrams – they do not grant lengthy analysis of imprecise nature of knowledge' (Stevens, 2011, p.9). Arguably, bearing in mind the forgoing remarks on the nature of policy-making operational-practice, the TCF could be a useful 'story telling' tool in the hands of policy makers. This specific usefulness of the TCF emphasises that a robust taxonomy in cybercrime scholarship is by no means a sign of regress but on the contrary, an indication of progress.

Furthermore, given that everyone who may be interested in cybercrime reports may not be an 'expert' in cybercrime, the TCF would provide a simplified tool of making sense of the complexities around the conceptualisation of cybercrime. Simply put, the TCF would have helped to showcase the statistical results of the ICCC's endeavours (and other cybercrime oriented undertakings) in a clearer light. In turn, it reinforces the elementary principles and the psychological benefits of categorisation (Rosch, 1978), which is central to the TCF. Therefore, the inability to differentiate between socioeconomic, geopolitical and psychosocial cybercrime is not a feature of the binary models alone: it limits the precision and clarity of ICCC's (2008–2010) reports as well. The crux is that the ICCC's umbrella term: 'cybercrime' or 'cybercrime perpetrators' is ambiguous and misleading at best.

It is not only misleading: it has consequences on the emerging academic discourse in Nigeria over the years. Specifically, it has influenced the framing of most scholarly endeavours in Nigeria (e.g. Adomi and Igun, 2008), which echo a sense of 'moral panic' on '419' phenomenon. Relatedly, the ICCC's reports could be implicated in supplying 'ammunitions' to 'Western propaganda machinery, which often blows the Nigerian 419 fraud-news out of proportion' (Adogame, 2007, p.7). Given that repeating discourses normalise their claim, the problem is deep. Whilst there is a total absence of social/contextual taxonomies in cybercrime scholarship, it is not difficult to notice the presence of 'league tables' as well as the binary models discussed above. This mismatch could be implicated in the uncritical representation of 'Nigeria as the third worst nation' in cybercrime literature (Aransiola and Asindemade, 2011; Adomi and Igun, 2008). Based on the premise that conceptualising cybercrime is challenging, this article therefore aims to stimulate contemporary scholarly endeavours from Nigeria and elsewhere to look beyond the 'league tables' and the binary models and consider contextual/social nuances at play. This is one of the usefulness of the TCF as it has the capacity to enable a clearer conceptualisation of cybercrime in Nigeria and beyond.

Unlike geopolitical and psychosocial categories, socioeconomic cybercrime is prevalent in Nigeria. Bearing in mind that the recognition of the socio-cultural fabric elements of a given situation is at the core of this paper, reinforces its value. The over-reliance on the populist 'league table' and the binary models in cybercrime scholarship has led some authors (e.g. Adomi and Igun, 2008; Chawki et al., 2015b) to overlook jurisdictional cultures and nuances. It has possibly misled some people in policy arenas. As Lagazio et al. (2014) observed, the orchestration of the fear of cybercrime in itself stimulates over-spending on defense measures as strategic responses by various states. Hyped rates of cybercrime in Nigeria by various discourses (academic, media) framed with the limitations of the prevailing taxonomies above have possibly influenced people in policy-making arenas. These conditions could be implicated in having knock-on-effects as AllAfrica (2013) pointed out, on the rise of the Nigerian government's budgets/expenses on cyber security oriented issues. Bearing in mind that there is a general 'paranoia' on the social 'problem' of Nigerian criminals (e.g. Agozino, 2003; Adogame, 2007), the concerns of international communities could creep into regional policy responses against the cybercrime 'problem'. In turn, international communities' concerns help to stretch the already over-stretched Nigerian expenses on a wide spectrum of cybercrime problem. The TCF would not only help to question the taken-for-granted assumptions on Nigerian cybercriminals' position on the global map, but also help policy makers to funnel down resources to cope with the specific category where Nigeria is most vulnerable. The key point is that the benefits of the TCF in coping with the complexities around cybercrime conceptualisation, outweigh that of the prevailing cybercrime taxonomies.

8. Historical perspectives: the Nigerian 419 fraud

Having problematised ICCC's (2006–2010) claim, it is worth considering the background to the Nigerian 419 fraud. 'Scam' is an age-old game in all human societies and the Nigerian 419 fraud, like its historical antecedents such as the Spanish Prisoner Swindle (Ogwezzy, 2012; Whitaker, 2013), has emerged from a particular history. Therefore, to dismiss long-term historical perspectives is vulnerable to omit critical factors necessary to understand the social and contextual platforms on which '419 fraud' has emerged. The underlying idea is to further develop the socioeconomic theory of Nigerian cybercriminals – answer to the question, what is cybercrime in Nigeria? Historically, socioeconomic cybercrime in contemporary Nigerian society metamorphised as Igwe (2007) narrated, from various types of deceptive 'games' played in pre-colonial Nigeria. Like all human societies, the contemporary Nigerian society that has sprouted from the ruins of three ancient West African

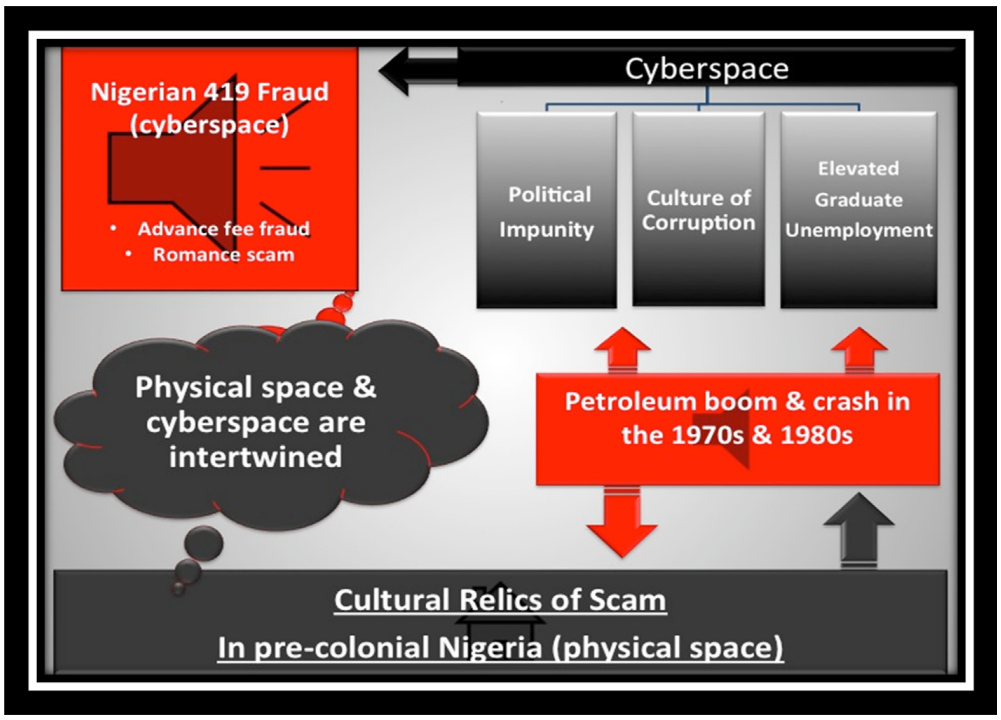


Fig. 3. Cultural relics of scam.

kingdoms: Benin kingdom, Bornu empire, and Songhai empire, (Shuter, 2008) has not done away with the relics of scam. Such scam-games of pre-colonial Nigeria are called *the ancient relics of scam*, as illustrated in Fig. 3 below. These relics of scam may be conceptualised as ancient assemblages of beliefs and practices that have evolved over time and entangled with the contemporary Nigerian democracy and politics, to become a common 'toolbox' for money success. Drawing from Robinson and McAdams (2015), in order to communicate this theoretical position beyond abstraction, the relics of scam hypothesis is simplified down to a set of verbal postulates, a box-and-arrow diagram – as illustrated in Fig. 3 below. One of the primary rationales being to enhance our understanding with the least cognitive effort. During the colonial period in Nigeria, whilst some commentators observed that 'crime' made little appeal to young Nigerians (e.g. Paterson, 1944), others noticed that Nigerian schoolboys were very gifted in the psychology of manipulations (e.g. US Consulate 1949). It could be that the former were referring to the general population of Nigerian youth, whereas the latter were referring to a specific group of young Nigerians – those who had the opportunity to embrace Western education in the 1940s. Besides, a majority of these reports on schoolboys were generated directly from their head teachers. The key point is that 'schoolboys' rather than 'illiterates' were principally implicated in authoring various kinds of letters, claiming as Ellis (2016) commented, to be sellers of diamonds, ivory, gold, and other exotic items from 'Africa', whereas they were the '*Wayo trickers*' – fraudsters. However, the 'destiny' of '*Wayo trickers*' changed drastically when petroleum was found in Nigeria (Adogame, 2007).

Petroleum was discovered in Nigeria four years prior to the official end of colonial rule in 1960. Consequently, petroleum became the dominant pillar of the Nigerian economy (Adogame, 2007). In turn, as Saro-wiwa (1989, p.21) commented, most political elites saw the oil-money as 'a national cake, already baked, ready to be shared'. For them, ruling the nation has nothing to do with nation-building but has everything to do with the funneling of federal money into personal bank accounts. While corruption is a global phenomenon, there is a long-standing view that Nigeria is not one of the 'cleanest' nations in the world (Transparency International, 2014). Although the petroleum boom has boosted the magnitude of corrupt practices in Nigeria, it also has some benefits.

As Smith (2008) described, the Nigerian petroleum boom was responsible for boosting the fertility rate as well as increasing the inflow of foreign scholars and workers in the 1970s. Consequently, numbers of educated people in Nigeria increased massively. However, nothing lasts indefinitely, and in the 1980s the price of oil fell drastically, rapidly deflating the Nigerian economy, but not corrupt practices. As oil boom became oil doom, the International Monetary Fund (IMF) entered the equation. To paraphrase Adogame (2007, p.8) 'IMF by prescribing deregulation exercises, austerity measures as the only panacea to economic reconstruction, ensnared Nigeria into a vicious circle of perpetual money borrowing and interest paying'. The misappropriation of these loans further deteriorated the economy. This was how the IMF, [9]corrupt practices of some politicians and political impunity became hopelessly interwoven with 419 fraud.

[9] For example, General Sanni Abacha, Nigerian president from 1993 to 1998 corruptly amassed a personal wealth of up to 4 billion USD (Igwe, 2007).

Specifically, Apfer (1999), in his analysis of 'IBB = 419', elaborated that, under General Ibrahim Badamasi Babangida (a.k.a. IBB), the longest-serving Nigerian Military regime (1985–1993) supported 419 kingpins and benefited directly from them. IBB's alleged elevated bribery-corruption scheme, political impunity and a range of kickbacks between other politicians and some foreign companies created real-life 'scripts', which added layers of authenticity to early 419 criminals' schemes. These layers of authenticity made the Nigerian 419 fraud templates invaluable/attractive to swindlers – Nigerians and non-Nigerians. It is easier for swindlers to modify/use the 'authentic' templates with track record of success, than to reinvent the wheel of the game. In other words, many of the fraud templates originated from plausible, or even genuine, crime scenarios. Evidently, as Adogame (2007) and Bretton (1962) observed, whilst numerous foreign companies found bribery and falsifying of paper work as keys to benefit from Nigeria, the politicians saw foreigners as a means of acquiring abundant wealth. The marriage between them over the years has produced voluminous '419 fraud templates' and reinforces the idea that cyber-crime in Nigeria is rooted in socioeconomics. As a result therefore of a sequence of events that interpenetrate one another to worsen the state of the economy, unemployed graduates, predominantly male, became a part of the equation.

Given the condition of the Nigerian economy in the 1980s, it was not difficult for most unemployed graduates to become vulnerable to 419 scamming (e.g. Adogame, 2007; Smith, 2008). It could be that the petroleum boom in the 1970s provided an elevated aspirational-level for university students. In consequence, higher expectations made the acceptance of unemployment-induced destitution 'harder' for recent graduates than for control groups, that is, average unemployed individuals. This echoes the discrepancy theory of satisfaction (Michalos,1985) in positive psychology, which postulates that upward social comparisons create a discrepancy between expectations and actual life events – upward social comparisons are most likely to stimulate lesser rather than greater satisfaction (see also Cooper and Artz, 1995; Perales and Tomaszewski, 2015).

The 'gap' or discrepancy between expectations and actual rewards chiefly determines whether people have low or high levels of satisfaction (Michalos, 1985; Cooper and Artz, 1995). However, this is not to concede that there is a causal relationship between unemployment and offending rates. The links between them despite showing some fairly clear patterns, are far from straightforward (e.g. Newburn, 2016). The most consistent view is that online crimes (as well as terrestrial crimes) in Nigeria are male dominated (e.g. Ojedokun and Eraye, 2012; Aransiola and Asindemade, 2011). This is important because male domination of cyber-fraud in Nigeria is linked to the socioeconomic cybercrime theory of Nigerian cyber-criminals, which, in turn, suggests fundamental problems with the prevailing binary category of cybercrime.

9. Socio-fabric elements and cultural landscapes

The explanations as to why adult males in Nigeria have been implicated in the bulk of socioeconomic cybercrime demands the application of cultural insights. The rationale being that there is an intersectionality of issues of interpersonal relationships in physical spaces and cyberspace. Cultural constellations of people in social contexts affect people's activities in cyberspace. The centrality of socioeconomic cybercrime in Nigeria is linked to the centrality of the patriarchal system. As Ibrahim (2015) pointed out, the strong patriarchal system and customary 'common-sense' in Nigeria among other factors, encourage men culturally, unlike women, to be the breadwinners. Due to men's cultural positionality in society in relation to women, men are generally more 'desperate' to achieve financial success. Indeed, contemporary scholars articulate that some cyber-criminals in the Sub-Saharan region go as far as deploying mystical/spiritual powers to enhance their exploits online (e.g. Tade, 2013 in Nigeria; Armstrong, 2011 in Ghana). The key point here is that regarding cybercrime, the primary aims of most Nigerian cyber-criminals converge on defrauding as many victims as possible (Smith, 2008; Akpome, 2015), which is illustrative of socioeconomic cybercrime, rather than for example, psychosocial cybercrime (please see Table 2 for victim-perpetrator primary and secondary loss/benefits).

One of the considerations that shape this trend is the local philosophy and demonstrable reality that, if a man is financially successful, he has 'unlimited' privileges in multiple facets of life-domains, unlike in Western society. For example, a man who has the means, regardless of his age, under customary and Islamic marriages can marry multiple wives. He can even marry wives as young as fourteen or thirteen years old, in some cases, depending on his 'tastes' (Nigerian Marriage Act, 1990; Ogunde, 2016; Monk et al. in press). Apart from the Nigerian common-sense custom allowing polygamy, a man's adultery is socio-culturally perceived as 'a heroic feat' (Chinwuba, 2015, p.305). These types of relationships shapes the manner in which a given society perceives its adult females at a particular historical point in time and how women are expected to relate to adult males (Ajayi and Owumi, 2013; Ibrahim, 2015; Chinwuba, 2015; Ogunde, 2016). It also extends to future generations and impacts on the children - *the* [10]*image-of-childhood* in the Sub-Saharan region (Rwezaura, 1998; Ibrahim and Komulainen, 2016). A strong patriarchal system helps to perpetuate these types of cultural landscapes, which in turn shape the socio-economic crime in Nigeria. Unlike in some Western nations, the cultural landscapes inherent in Nigeria invoke relatively positive societal reactions, towards any man who has financial success (irrespective of the source of such a success – e.g. cyber-fraud) (see also Becker, 1967 on social reactions). Such background evidence reinforces that the Nigerian cyber criminals' are primarily monetary-driven as illustrated in Table 2. Therefore, the Nigerian cybercriminals (popularly ranked third)

[10] The 'image-of-childhood' refers broadly to the manner in which a given society perceives its children at a particular historical point in time and how children are expected to relate to the adult world (Ibrahim and Komulainen, 2016).

are under one nuanced umbrella of cybercrime – cyber-fraud (socioeconomic cybercrime), which is not made clear through the lens of the binary model as the well as ICCC's (2008–2010) observations.

The above social and contextual factors informed the core of present day cybercrime in Nigeria. Arguably, these forms of cultural landscapes are possibly the explanations for the centrality of socioeconomic cybercrime in Nigeria, which suggests problems with the existing binary model of cybercrime as aforementioned. The implication is that what is cybercrime in Britain or in the USA - ranked second and first respectively, (ICCC, 2010) does not fit squarely within the contextual meaning of cybercrime in Nigeria. For instance, unlike the Sub-Saharan region, as Sheridan et al. (2014) pointed out, in most Western nations, cyber stalking is a social problem. Another implication is that these social and contextual factors also challenge the simplistic rendering of cyberspace and physical space as two different entities with easily defined boundaries as they are intertwined, as shown in Fig. 3. Evidently, the particularities of cybercrime in Nigeria support the incorporation of social and contextual factors into cybercrime classifications and consequently, render problematic the existing taxonomies.

10. Conclusion

This article has aimed to establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrime. It has examined the explanatory capacity of the existing taxonomies in making sense of what is true of all societies, and what is true of one society at one point in time and space. Thus, these analyses have helped to propose that whilst in Nigeria, cybercrime is fundamentally rooted in socioeconomics, the lenses of the existing cybercrime taxonomies are not well equipped to project the pattern of this phenomenon clearly. Therefore, in line with motivational theories framed within the basic psychological framework of categorisation, this paper has not only complemented the existing taxonomies, but has also offered a more conceptually robust alternative for grouping cybercrime: the TCF. It has argued that cybercrime can be motivated three possible ways: socioeconomic, psychosocial and geopolitical. Whilst what constitutes cybercrime in most Western nations such the UK and the USA may involve these three groups, cybercrime in Nigeria is fundamentally rooted in socioeconomics. Therefore, the conceptual 'pipelines' of the cybercrime framework in the Global North may not hold water in Nigeria – representing the Sub-Saharan region. Drawing together and extending categories of cybercrime, this article has provided a more holistic taxonomy incorporating socioeconomic, psychosocial and geopolitical motivations. This contribution offers new ways of making sense of numerous variances of cybercrime listed in Table 1. It also provides a clearer way of conceptualising cybercrime in Nigeria and elsewhere because jurisdictional cultures and nuances apply online as they do offline.

Acknowledgment

I am grateful to Professor Robert Reiner and Dr Jessica Morgan for their comments on my draft, and I also thank the anonymous reviewers for their insightful and thoughtful comments. I thank my friends, Nicola Baldwin, Shervin Vencatachellum, Andreas Haggman and Stephen Wyatt, for proofreading different parts of my draft and Dr Laura Christie for proofreading the final version of this article as a whole. I am grateful to the journal's production manager (Sneha Mohan) for her patience. I also thank the organisers and participants of the 4th International Conference on Cybercrime & Computer Forensics – Vancouver, where I presented this paper in June 2016 (at Simon Fraser University). My sincere gratitude goes to my mentor, Professor Ravinder Barn, for her comments when I was working under her (The CyberRoad Map Project from 2014 to 2015); a fragment of this paper was my unpublished contribution to the Project. I also thank the EPSRC and the UK government as part of the Center for Doctoral Training in Cyber Security at Royal Holloway, University of London.

References

Adogame, A., 2007. The 419 code as business unusual: youth and the unfolding of the advance fee fraud online discourse. Int. Sociol. Assoc. e-bull. http://www.isa-sociology.org/publ/e-bulletin/E-bulletin_7.pdf (accessed 10.07.16.).
Adomi, E.E., Igun, S.E., 2008. Combating cyber crime in Nigeria. Electron. Libr. 26 (5), 716–725 (Emerald Publishing).
Agozino, B., 2003. Counter-colonial Criminology: a Critique of Imperialist Reason. Pluto Press, London.
Ajayi, J., Owumi, B., 2013. Socialization and child rearing practices among nigerian ethnic groups. Acad. J. Interdiscip. Stud. 2 (2), 249–256.
Akpome, A., 2015. What is Nigeria? unsettling the myth of exceptionalism. Afr. Spectr. 50 (1), 65–78.
AllAfrica, 2013. Nigeria: Budget - Security Vote Shoots up to N1 Trillion. available at: http://allafrica.com/stories/201210151017.html (accessed 11.05.16.).
Apfer, A., 1999. IBB=419: nigerian democracy and the politics of illussion. In: Comaroff, John, Comaroff, John (Eds.), Civil Society and the Political Imagination in Africa: Critical Perspectives. University of Chicago Press, Chicago.
Aransiola, J.O., Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychology, Behav. Soc. Netw. 14 (12), 759–763.
Armstrong, A., 2011. 'Sakawa' Rumours: Occult Internet Fraud and Ghanaian Identity (No. 8). UCL [online]. https://www.ucl.ac.uk/anthropology/research/working-papers/082011.pdf (accessed 11.02.16.).
Balancing Act, 2014. Nigeria Ranked Third in the World for Cybercrime. available at: http://www.balancingact-africa.com/news/en/issue-no-302/computing/nigeria-ranked-third/en (accessed 30.05.16.).
Benson, V., Saridakis, G., Tennakoon, H., 2015. Purpose of social networking use and victimisation: are there any differences between university students and those not in HE? Comput. Hum. Behav. 51, 867–872.
Bohme, R., Moore, T., 2012. How do consumers react to cybercrime?. In: eCrime Researchers Summit (ECrime), 2012, pp. 1–12. IEEE Xplore.
Boulton, M., Lloyd, J., Down, J., Marx, H., 2012. Predicting undergraduates' self-reported engagement in traditional and cyberbullying from attitudes. Cyberpsychology, Behav. Soc. Netw. 15 (3), 141–147.
Brathwaite, F., 1996. Some aspects of sentencing in the criminal justice system of Barbados. Caribb. Quart 42 (2/3), 101–118.
Brenner, S.W., 2007. Cybercrime: Re-thinking crime control strategies. In: Jewkes, Y. (Ed.), Crime Online. Willan, Cullompton, pp. 12–28.

Brenner, S.W., 2012. Cybercrime and the Law: Challenges, Issues, and Outcomes. Northeastern University Press, New England.
Bretton, H.L., 1962. Power and Stability in Nigeria: the Politics of Decolonization. Frederick A. Praeger, London.
Brown, K.V., 2001. The determinants of crime in South Africa. South Afr. J. Econ. 69 (2), 269–298.
Cain, M., 2000. Orientalism, occidentalism and the sociology of crime. Br. J. Criminol. 40 (2), 239–260.
Chawki, M., Darwish, A., Khan, M.A., Tyagi, S., 2015a. Cybercrime: introduction, motivation and methods. In: Cybercrime, Digital Forensics and Jurisdiction. Springer International Publishing, pp. 3–23.
Chawki, M., Darwish, A., Khan, M.A., Tyagi, S., 2015b. 419 scam: an evaluation of cybercrime and criminal code in Nigeria. In: Cybercrime, Digital Forensics and Jurisdiction. Springer International Publishing, pp. 129–144.
Chinwuba, N.N., 2015. Human identity: child rights and the legal framework for marriage in Nigeria. Marriage & Fam. Rev. 51 (4), 305–336.
Cooper, A.C., Artz, K.W., 1995. Determinants of satisfaction for entrepreneurs. Journal of Business Venturing 10 (6), 439–457.
Csikszentmihalyi, M., 1990. Flow: the Psychology of Optimal Experience. Harper and Collins, New York.
Csikszentmihalyi, M., 2000. Beyond Boredom and Anxiety: Experiencing Flow in Work and Play, second ed. Jossey Bass, San Francisco.
Csikszentmihalyi, M., 2014. Toward a psychology of optimal experience. In: Flow and the Foundations of Positive Psychology. Springer, Netherlands, pp. 209–226.
Cunningham, C.E., Chen, Y., Vaillancourt, T., Rimas, H., Deal, K., Cunningham, L.J., Ratcliffe, J., 2014. Modeling the Anti-cyberbullying Preferences of University Students: Adaptive Choice-based Conjoint Analysis. Aggressive behavior.
Deci, E.L., Ryan, R.M., 1985. Intrinsic Motivations and Self-determination in Human Behaviour. Plenum, New York.
Deci, E.L., Ryan, R.M., 2000. The 'what' and 'why' of goal pursuits: human needs and the self-determination of behaviour. Psychol. Inq. 11 (4), 227–268.
Deci, E.L., Ryan, R.M., 2011. Self-determination theory. Handb. Theor. Soc. Psychol. 1, 416–433.
Doyon-Martin, J., 2015. Cybercrime in West africa as a result of transboundary e-waste. J. Appl. Secur. Res. 10 (2), 207–220.
Ellis, S., 2016. This Present Darkness: a History of Nigerian Organized Crime. Oxford University Press, Oxford.
Farrell, G., 2010. Situational crime prevention and its discontents: rational choice and harm reduction versus 'cultural criminology'. Soc. Policy & Adm. 44 (1), 40–66.
Faucher, C., Jackson, M., Cassidy, W., 2014. Cyberbullying Among University Students: Gendered Experiences, Impacts, and Perspectives, vol. 2014. Education Research International.
FBI, 2014. African Cybercriminal Enterprise Members Using School Impersonation to Defraud Retailers. available at: http://www.ic3.gov/media/2014/140904.aspx (accessed 30.05.16.).
FBI, 2015. Mission Statement. available at: https://www.ic3.gov/about/default.aspx (accessed 28.05.16.).
FBI, 2016. Internet Crime Schemes. available at: https://www.ic3.gov/crimeschemes.aspx#item-13 (accessed 27.05.16.).
Gordon, S., Ford, R., 2006. On the definition and classification of cybercrime. J. Comput. Virol. 2 (1), 13–20.
Hayward, K., 2007. Situational crime prevention and its discontents: rational choice theory versus the 'culture of now'. Soc. Policy & Adm. 41 (3), 232–250.
Ibrahim, S., 2015. A binary model of broken home: parental death-divorce hypothesis of male juvenile delinquency in Nigeria and Ghana. In: Maxwell, S.R., Blair, S.L. (Eds.), Violence and Crime in the Family: Patterns, Causes, and Consequences, Contemporary Perspectives in Family Research, vol. 9. Emerald Group Publishing Limited, New York, pp. 311–340.
Ibrahim, S., Komulainen, S., 2016. Physical punishment in Ghana and Finland: criminological, sociocultural, human rights and child protection implications. Int. J. Hum. Rights Const. Stud. 4 (1), 54–74.
Ibrahim, S., 2016. Causes of Socioeconomic Cybercrime in Nigeria (Parents' Perspectives). The 4th International Conference on Cybercrime & Computer Forensics. IEEE Xplore Publishing, Canada, Vancouver.
Igwe, C.N., 2007. Taking Back Nigeria from 419: what to Do about the Worldwide E-mail Scam–advance-fee Fraud. iUniverse, Toronto.
Internet Crime Complaint Centre – ICCC (2006), 'Internet Crime Complaint Centre', available at: https://pdf.ic3.gov/2006_IC3Report.pdf, (accessed 04.04.15.).
Internet Crime Centre Complaint Centre – ICCC (2008) 'Internet Crime Centre Complaint Centre', available: https://pdf.ic3.gov/2008_IC3Report.pdf, (accessed 27.05.16.).
Internet Crime Centre Complaint Centre – ICCC (2009) 'Internet Crime Centre Complaint Centre', available at: https://pdf.ic3.gov/2009_IC3Report.pdf, (accessed 28.05.16.).
Internet Crime Centre Complaint Centre – ICCC (2010) 'Internet Crime Report', available at: https://pdf.ic3.gov/2010_IC3Report.pdf, (accessed 26.05.16.).
Internet Crime Centre Complaint Centre – ICCC (2011) 'Internet Crime Report', available at: https://www.its.ny.gov/sites/default/files/documents/2011_IC3Report.pdf, (accessed 29.05.16.).
Internet Crime Centre Complaint Centre – ICCC (2012) 'Internet Crime Report', available at: https://pdf.ic3.gov/2012_IC3Report.pdf, (accessed 29.05.16.).
Internet Crime Centre Complaint Centre – ICCC (2013) 'The Internet Crime Centre Report 2013', available at: https://pdf.ic3.gov/2013_IC3Report.pdf, (accessed 27.05.16.).
Internet Crime Centre Complaint Centre – ICCC (2014) 'The Internet Crime Centre Report 2014', available at: https://pdf.ic3.gov/2014_IC3Report.pdf, (accessed 27.05.16.).
Kaspersky, 2016. The Overall Statistics for 2015. available at: https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/ (accessed 09.01.16.).
Kshetri, N., 2006. The simple economics of cybercrimes. Secur. Priv. IEEE 4 (1), 33–39.
Lagazio, M., Sherif, N., Cushman, M., 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector. Comput. Secur. 45, 58–74.
Layous, K., Nelson, S.K., Lyubomirsky, S., 2013. What is the optimal way to deliver a positive activity intervention? the case of writing about one's best possible selves. J. Happiness Stud. 14 (2), 635–654.
Lazarus, R.S., 2006. Stress and Emotion: a New Synthesis. Springer Publishing Company.
Lazarus, R., Folkman, S., 1984a. Stress, Appraisal and Coping. Springer, New York.
Lazarus, R., Folkman, S., 1984b. Stress, Coping and Adaptation. Springer, New York.
Lindsay, M., Krysik, J., 2012. Online harassment among college students: a replication incorporating new Internet trends. Inf. Commun. Soc. 15 (5), 703–719.
Longe, O.B., Mbarika, V., Kourouma, M., Wada, F., Isabalija, R., 2010. Seeing beyond the surface, understanding and tracking fraudulent cyber activities arXiv preprint arXiv:1001.1993.
Manjikian, M.M., 2010. From global village to virtual battlespace: the colonizing of the internet and the extension of realpolitik. Int. Stud. Quart 54 (2), 381–401.
McGuire, M., Dowling, S., 2013. Cyber crime: A review of the evidence. available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (accessed 28.09.14.).
Michalos, A., 1985. Multiple discrepancies theory (MDT). Soc. Indic. Res. 16, 347–413.
Monk, C., Ibrahim, S., Rush, M., Dibiana, E. T, 2016. Unequal sociocultural penalties of divorce in Nigeria and citizenship implications. Special issue. J. Comp. Fam. Studies (in press).
Nakamura, J., Csikszentmihalyi, M., 2002. The concept of flow. In: Snyder, C.R., Lopez, S.J. (Eds.), Handbook of Positive Psychology. Oxford University Press, New York, pp. 89–105.
Nelken, D., 2010. Comparative Criminal Justice: Making Sense of Difference. SAGE, London.
Newburn, T., 2016. Social disadvantage: crime and punishment. In: Dean, H., Platt, L. (Eds.), Social Advantage and Disadvantage. Oxford University Press, Oxford.
Nigerian Marriage Act, 1990. Marriage Act. available at: http://www.placng.org/new/laws/M6.pdf (accessed 22.01.16.).
Ogunde, O., 2016. Protecting the interest of the girl-child in Nigeria: matters arising. Int. J. Hum. Rights Const. Stud. 4 (1), 17–30.

Ogwezzy, M.C., 2012. Cyber crime and the proliferation of yahoo addicts in Nigeria. AGORA Int. J. Jurid. Sci. 1, 86–102.
Ojedokun, U.A., Eraye, M.C., 2012. Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. Int. J. Cyber Criminol. 6 (2), 1001–1013.
Oksanen, A., Keipi, T., 2013. Young people as victims of crime on the internet: a population-based study in Finland. Vulnerable Child. Youth Stud. 8 (4), 298–309.
Paterson, A., 1944. National Archives of Nigeria, Ibadan, Oyo Prof.1, 4113: "Crime and its Treatment" report to the Governor by Alexander Paterson, February 1944.
Perales, F., Tomaszewski, W., 2015. Happier with the same: job satisfaction of disadvantaged workers. British Journal of Industrial Relations. http://espace.library.uq.edu.au/view/UQ:341908/UQ341908_OA.pdf.
Reiner, R., 2010. The Politics of the Police. Oxford University Press, Oxford.
Robinson, O.C., McAdams, Dan P., 2015. Four functional roles for case studies in emerging adulthood research. Emerg. Adulthood 3 (6), 413–420.
Rosch, E., 1978. Principles of categorization. In: Rosch, Eleanor, Lloyd, Barbara B. (Eds.), Cognition and Categorization 27–48. Lawrence Erlbaum, Hillsdale, NJ.
Rwezaura, B., 1998. Competing 'images' of childhood in social and legal systems of contemporary Sub-Saharan Africa. Int. J. Law Policy Fam. 12 (3), 253–278.
Saro-wiwa, K., 1989. On a Darkling Plain: an Account of the Nigerian Civil War. Saros International Publishers, Port Harcourt.
Sheridan, L., Scott, A.J., Nixon, K., 2014. Police Officer Perceptions of Harassment in England and Scotland. Legal and Criminological Psychology.
Shuter, J., 2008. Ancient West African Kingdoms. Heinemann Educational Books, London.
Smith, D.J., 2008. A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria. Princeton University Press, Princeton.
Stevens, A., 2011. Telling policy stories: an ethnographic study of the use of evidence in policy-making in the UK. J. Soc. Policy 40 (02), 237–255.
Tade, O., 2013. A spiritual dimension to cybercrime in Nigeria: the 'yahoo plus' phenomenon. Hum. Aff. 23 (4), 689–705.
Tade, O., Aliyu, I., 2011. Social organization of internet fraud among university undergraduates in Nigeria. Int. J. Cyber Criminol. 5 (2), 860–875.
Transparency International, 2014. The 2014 Corruption Perception Index. Available at. http://www.transparency.org/cpi2014. accessed 30.12.15.
US consulate, 1949. NARA II RG 84, records of the US consulate, Lagos, 1940 to 1963 Box 1: C. Porter Kuykendall, consul-general, to Secretary of State, 16 May 1949.
Wall, D.S., 2008. Cybercrime and the culture of fear: social science fiction (s) and the production of knowledge about cybercrime. Inf. Commun. Soc. 11 (6), 861–884.
Wall, D.S., 2013. Cybercrime, 2007. Polity Press, Cambridge.
Wehmeyer, M., Little, T., 2009. Self-determination. In: Lopez, S. (Ed.), Encyclopedia of Positive Psychology. Blackwell Publishing Ltd, Chichester, pp. 868–874.
Whitaker, R., 2013. Proto-Spam: Spanish prisoners and confidence games. Appendix 1 (4) available at: http://theappendix.net/issues/2013/10/proto-spam-spanish-prisoners-and-confidence-games (accessed 12.12.15.).
Yar, M., Jewkes, Y., 2010. Histories and Contexts. Handbook of Internet Crime. Routhledge Books, London.
Yazdanifard, Rashad, Oyegoke, Tele, Seyedi, Arash Pour, 2011. Cyber-crimes: Challenges of the Millennium Age." Advances in Electrical Engineering and Electrical Machines. Springer, Berlin Heidelberg, pp. 527–534. http://link.springer.com/chapter/10.1007/978-3-642-25905-0_68 (accessed 30.03.15.).

Causes of Socioeconomic Cybercrime in Nigeria

(Parents' Perspectives)

Suleman IBRAHIM
The Centre for Doctoral Training in Cyber Security
The Information Security Group
Royal Holloway University of London
TW20 0EX Surrey, UK
suleman.ibrahim.2014@live.rhul.ac.uk

Abstract— The causations of crimes that are relevant in the cyberspace concurrently impact in the physical space and vise versa. This paper aims to explore parents' perceptions of the factors that cause socioeconomic cybercrime in Nigeria. Despite a long-standing view that the juvenile offenders of today could become the hardened criminals of tomorrow, and the conclusions of a number of developmental theories on the stability of delinquency across the life course, the existing data on cybercrimes in Nigeria have principally been derived from studies involving university students. Yet, individuals' moral-standard-levels, which shape their offending capacities, are mostly developed in childhood. The empirical basis for this paper is face-to-face interviews with 17 Nigerian parents regarding children's vulnerability to involvement in cybercrime. Drawing upon qualitative data, this paper argues that a complex web of familial factors and structural forces, alongside cultural forces, explains the degree of cybercrime involvement on the part of Nigerian youths.

Keywords—Socioeconomic cybercrime; Nigerian 419 fraud, Area Boys, Yahoo Boys, juvenile delinquency; family factors, corruption, cyber criminology.

I. INTRODUCTION

Nigeria is an Anglophone Sub-Saharan nation, surrounded by Francophone nations and the Gulf of Guinea. Despite having over two hundred ethnic variations, speaking numerous languages, it uses English as its official language due to colonialisation by the British [1]. As a result, pidgin English generally serves as a lingua franca for most Nigerians [2]. Nigeria is seen as the third worst country globally when it comes to the prevalence of cybercrime perpetrators [3]. However, the cybercrime 'league tables' are problematic, because the statistics relied on to inform the prevalence of cybercrime perpetrators across nations are socially and selectively constructed [4]. The Internet Crime Complaint Centre's [3] 'league tables' are merely pictorial representations of that construction [4]. The most consistent view is that young adult males have been implicated in the bulk of online criminal activities [2], [4], especially socioeconomic cybercrime, locally known as [1]419 crimes in Nigeria [5]. Socioeconomic cybercrimes may be conceptualised as intentional fraud-based crimes that are computer or/and internet-mediated, such as cyber fraud, romance scams, and e-embezzlement. Therefore, 'cybercrime[2]' in the Federal Republic of Nigerian is rooted in socioeconomics [4]. This paper aims to explore parents' perceptions of the factors that cause socioeconomic cybercrime in Nigeria, and argues for the need to consider juvenile delinquency as a contributory factor.

The term juvenile delinquency is socio-culturally constructed [6] yet numerous researchers such as Farrington [7], Loeber et al. [8] and Moffitt [9] have broadly defined it as a set of law-breaking behaviors. This current paper agrees with the above authors' definitions of juvenile delinquency. The family is crucial in shaping children's behavior [10]. Yet, as Belsky and Jaffee [11] pointed out, the success of good parenting depends on environmental forces, familial factors and children's individual characteristics. Building upon Belsky and Jaffee's [11] idea, Ibrahim's [12] analysis of cultural penalties of divorce in Nigeria/Ghana categorised juvenile delinquency risk factors into tripartite branches as illustrated in Fig. 1.

In Nigeria, however, there has historically been a total absence of empirical study on juvenile delinquency, up until official colonialisation ended in 1960 [13]. Whilst juvenile delinquency has been extensively investigated in the Global North, studies based on Sub-Saharan nations are scanty [12], [14]. In part, what one quickly notices is that, numerous studies conducted in Western societies have examined individual, familial and structural factors, whereas familial factors exclusively dominate most Nigerian studies on juvenile delinquency [12]. The centrality of family and the notion of 'family name' are also critical socio-cultural explanations for this paradigm in Nigerian literature [15]. For Ebbe [15, pp.356], 'family-name',

[1] "419 is "coined from section 419 of the Nigerian criminal code dealing with fraud. Nowadays, the axiom '419' generally refers to a list of offences [such as] stealing, cheating, falsification, impersonation, counterfeiting, forgery and fraudulent representation of facts [5, pp. 129].

[2] The term 'cybercrime' in this article means: socioeconomic cybercrime.

is culturally perceived as supreme in Nigeria, and must be protected more than members' rights and tendencies.

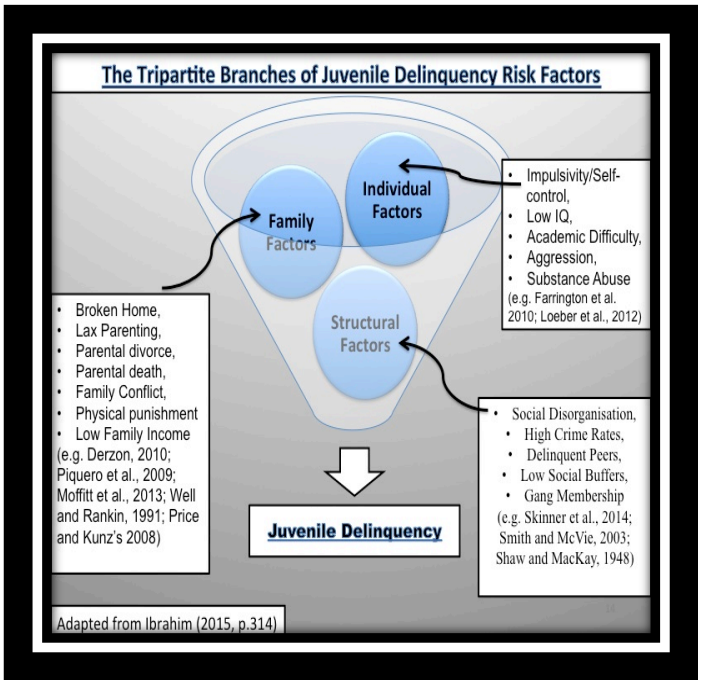


Fig. 1: The Tripartite Branches of Juvenile Delinquency Risk Factors

The cultural meaning of 'family-name' is indicative of the centrality of the family as a major determinant of children's behavior in this region. Thus, centrality of the family is crucial when considering cybercrime and/or terrestrial crime in Nigeria.

II. LITERATURE REVIEW

Whilst juvenile delinquency literature is primarily concerned with terrestrial crimes, the cybercrime literature is focused, as its name implies, on digital crimes. The majority of Nigerian literature on juvenile delinquency concentrates primarily on children from about 13-18 years [15], [16], [17], whereas most Nigerian literature on cybercrime focuses principally on university students [18], [19], [20]. The different patterns of existing data in these two paradigms have led to different assertions. Specifically, whilst Sanni et al. [17, pp. 27] in looking at juvenile delinquency pointed out that a "healthy home environment is the single most important factor necessary to keep children from becoming delinquent", Aransiola and Asindemade [18, p.762] in examining cybercrime concluded that, "higher institutions of learning in Nigeria serve as the breeding grounds for cybercriminals". The convergence of Nigerian data on cybercrime has ignored the cybercrime breeding factors in these criminals' childhood lives, whereas the literature on juvenile delinquency has lost sight of the centrality of the 'cybercrime phenomenon' in the lives of young adults in Nigeria. A person's family home existed before that person's university-environment: the relationship between the two is worth focusing on. Therefore, the overarching question is, what are parents' perceptions of the causes of cybercrime involvement among Nigerian children? One possible explanation for the disjunction between research on cybercrime and research on juvenile delinquency could be located in the absence of longitudinal studies in Nigeria and the African continent as a whole (apart from the recent scholarly endeavor in Ethiopia, a longitudinal study called Young Lives, by Virginia Morrow and colleagues).

This suggests that, in terms of cybercrime, limited studies have investigated the early risk factors. To paraphrase Kazdin et al. [21, pp.377], 'risk factors are associated with an increase in the probability (risk) of a particular outcome over the base rate of the outcome among control groups' (see also [22]). This present paper aims to fill this gap in the literature, by looking at risk factors that may influence Nigerian children's involvement in cybercrime. Unlike previous studies on cybercrime in Nigeria, this paper stresses the need to consider the role of the family in discouraging or encouraging cyber-criminality in children. University students have often been the focus of cybercrime literature in Nigeria. However, they have already developed their level of moral awareness before enrolling as university students. Support for this position on moral awareness is found in some studies, which have indicated that the behavior of adults is more stable than that of children [7], [9]. To this end, examining how the family environment could shape children's behavior could be more beneficial in understanding how to combat cybercrime than the more typical research focus on Nigerian universities as cybercrime breeding grounds. At this point, it is worth focusing on corruption, a key factor that promotes and sustains cybercrime in Nigeria.

A. Cybercrime and Corruption

Nigeria is not one of the 'cleanest' nations in the world [23] with some researchers claiming that Nigerian society is plagued with bribery and corruption [2], [4], [24]. Thus, it seems implausible that some agents of the state, such as the street-level police officers, would not be involved in illegal practices such as corruption. Empirical evidence of this is found in Aransiola and Asindemade's [18] study, which interviewed 40 cybercriminals in a Nigerian university. Specifically, the authors explained that, some street-level law enforcement officers act as informants to cyber-criminals in providing useful information that support their criminal activities. Some other scholars have also pointed out that some corrupt politicians have been implicated in using law enforcement agencies as political tools to oppress and intimidate their political opponents [25]. Therefore, the problem lies deep within Nigerian society. This type of predicament led some scholars to believe that the overall legal strategies adopted for fighting cybercrime were ineffective [5], [24]. Other scholars have also raised concerns that political impunity, bribery and corruption among representatives of authority have disoriented the moral compass of most everyday Nigerian civilians [2], [25]. Adeniran [25, p.11] elaborated that "[T]he value that [the Nigerian] society has placed on wealth accumulated has been a

potent determinant of youth involvement in online fraudulent practices". This paper aims to explore the role of corruption in propagating 419 cybercrime activities in Nigeria, from the perspective of parents.

III. Methods

Based on the themes evident in the existing literature, a flexible qualitative design was deployed. This design was geared to explore the experiences and perceptions of parents, who are in Code's [26] term, 'local-knowers', when it comes to children's involvement in cybercrime in Nigeria. This paper defines 'local-knowers' as Nigerians who have: [a] schooled, lived, and/or worked in Nigeria until their early thirties (before relocating to London, England) and [b] directly or vicariously experienced cybercrime in Nigeria (some of whom may or may not themselves have been perpetrators of cybercrime in Nigeria).

A. Participants Descriptions

In terms of demographics, out of the 17 respondents, 10 were male and 7 were female, with a mean age of 45 years. A majority of them had three children. Fourteen of the participants lived with a partner/wife/husband as well as their children, while three were single parents.

B. Data Collection

Snowball sampling was used to recruit participants. In-depth semi-structured interviews were used as a means of data collection [27], [28]. The researcher personally interviewed all seventeen[3] participants (in English as well as pidgin English), with interviews lasting from 50 to 70 minutes. All interviews were tape recorded with the consent of the interviewees. The importance of discussing the reasons for young people's involvement in cybercrime in Nigeria appears to have encouraged the participants to consent to the interviews.

C. Identification of Themes and Coding

The researcher's knowledge and personal ideas about the field were set aside to the extent possible, with the grounded coding approach of Ryan and Bernard [27] being applied to the data. As a result, new themes not found in the existing literature emerged (e.g. 'family related factors') alongside the existing ones (e.g. corruption). Finally, the researcher validated the emerged themes with 59% of the respondents, referred to as membership validation [29].

IV. FINDINGS

Based on the level of convergence in the respondents' reports (frequency) as illustrated in Figs. 2 and 3, family-related factors such as "a good family environment", parental supervision, and parental upbringing were the dominant ones in relation to other macro-level factors such as corruption.

A. A Good Family Environment

All interviewees (n=17) reported that a good family environment' is the most important factor in discouraging Nigerian children's involvement in cybercrimes. In fact, "a good family environment" was the main issue that all respondents most frequently discussed in-depth, regardless of the particularity of the researcher's questions or the specificity of the themes that were used as interview guides. Respondents generally perceived a good family environment as being the presence of a consistent and positive role model in children's lives. In the language of participant 2BM:

"*A child needs a good family environment. A good family environment is [a home] where the mother and the father are present in a child's life, you know...raising the child according to the values and culture or rather cultural beliefs of that family. A child [from a good family environment] tends to grow up well and behave well irrespective of bad things in society* [general societal decadence] *surrounding the family environment.*"

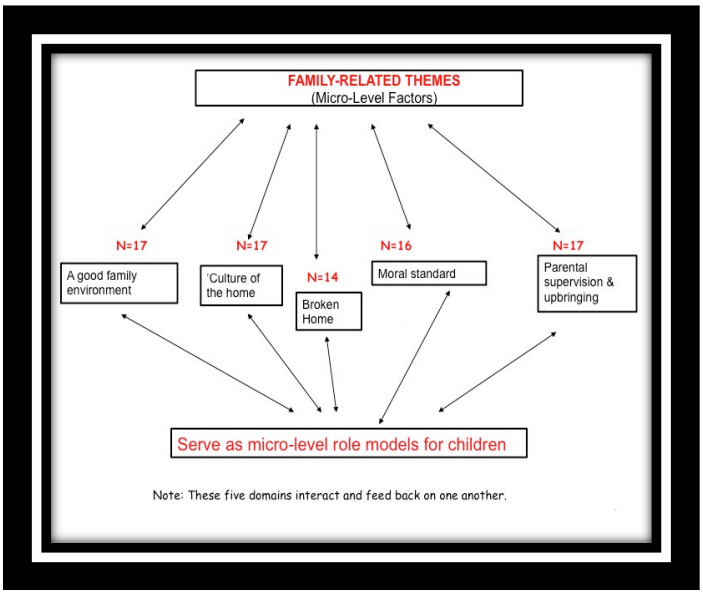


Fig. 2: Family Related Factors

A. Broken Home

[3] Twelve respondents were initially interviewed and analyzed. Five other respondents were interviewed two months later, but no new themes emerged from the second tranche of interviews.

Disrupted families and good family environments were perceived as being at the opposite ends of the continuum. Respondents felt that a good family environment was more likely to be attained in intact families than in non-intact homes. Support for the role of the 'broken home' in the family's well-being is evident in participant 8HS's report:

"*In a united family, where children have both parents, it is often difficult to find the children go astray…but in an unsettled home there is a tendency that the children always go astray morally and mentally. A single mother is always struggling to raise money from the market. [As a result, she] cannot be at home to watch [supervise her] children. Those children have the tendency to mix up with children from the gutter [have the tendency to mix up with delinquent peers*]".

B. Culture of the Home

Closely related to the above is what some participants called "culture of the home", which they explained was vital in the shaping of a child's overall behavior in terms of criminality in general. According to Participant 7GW:

"*Nigerian children are involved in 419 business due to bad culture. I mean the culture of the home, because every home has its own culture. If the immediate home of a child has lost its good cultural values… then the child can be involved in bad things like 419. As a child, the first point of call is the home: father and mother. An individual child is like a sheet of paper, it is what the parents write on it, that moulds the child's moral standard. That is why I said that it is the culture of the home that matters in Nigeria*".

C. Parental Upbringing

In a similar vein, the interviewees frequently mentioned the issue of parental upbringing (which has a strong correlation with a good family environment). It was felt that children from "a good family environment" were more likely to receive a good-quality parental upbringing than those from a disrupted family environment. As Participant 8HS stated:

"*Parental upbringing matters a lot in Nigeria. The bible says, 'train up a child the way he will grow up'. When you bring up your child with a high moral standard, there is every tendency that such a child will not go astray. Theoretically, if parents have a high moral standard, there is every tendency that the children will not have foreign characters [bad characters], because such parents will always question their children whenever they notice foreign character in them. For example, if you don't question children in Nigeria, that means you encourage them to get what I would like to call,…'an apprenticeship in 419 business' in later life".*

Also, closely related to 'parental upbringing' in Nigeria is 'family name', which is a principal driver of most child-rearing philosophies enunciated above [15]. The sociocultural fear about endangering one's family name acts as a crime deterrence mechanism. The Nigerian emphasis on family name is illustrated by the following comment from Participant 5EB:

"A good family personality [a good family name] serves as a constant reminder to children. I for one, there are certain things I wouldn't want to associate myself with, simply because it would break the heart of my family. [He looked very pleased with himself and continued] if you don't checkmate your children and ask them the right questions, what kind of seed are you sowing?".

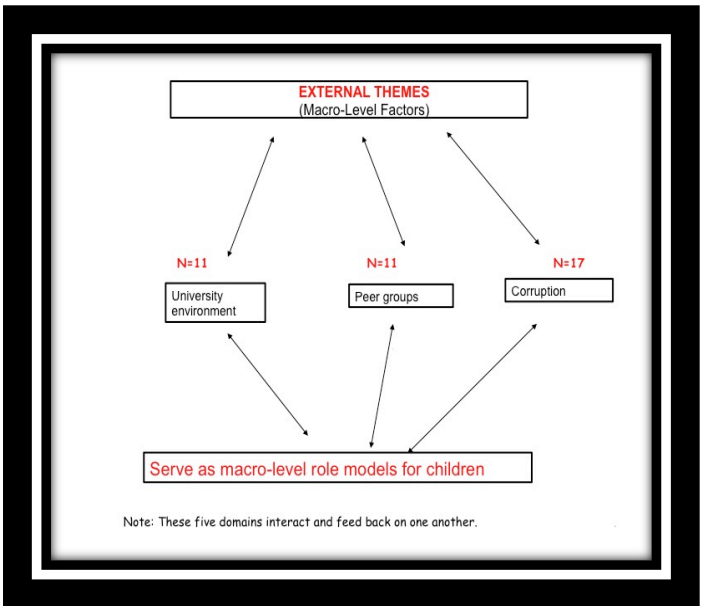


Fig. 3: External Factors

A. Corruption

Apart from familial factors, corruption in society was another issue that produced a very high degree of consensus, and was the second most frequently mentioned factor. This suggests that a link between corruption and family variables could be constructed, because a family does not exist in a vacuum, but in society. As Participant 10JB stated reported:

"Before we start pointing our hands to [the corrupt] Nigerian government, we have to look deep down in ourselves, our homes. The corrupt people in top places in Nigeria are from bad homes, it is bad people we have in various bad homes that make up a great percentage of bad government we have in Nigeria…. they preach one thing and practice another".

Additionally, other participants commented on corrupt practices among various authority figures in Nigeria, such as

the police officers. They reported that corruption in Nigeria is a major driver of cybercrime because four branches – police officers, politicians, bank officers and spiritualists, all agents of the state apparatus, often collaborate with cybercriminals.
"My sister used to own a restaurant in Lagos. One day, police arrested 419 guys who dey celebrate for my sister restaurant [police arrested some 419 guys who were celebrating in my sister's restaurant]*, but the following day, they returned like say nothing happened [but the following day, they returned to continue their celebration as if nothing had happened]. They boasted that they have settled the police, [bribed the police] that in fact it was a group of police officers who they did not settle [bribe], that came to the restaurant to crash their party*" (Participant 5AK).

"Bank workers play vital roles [too]. For example, you can imagine a jobless young man coming to banks to claim huge amounts of money regularly, without any interview; how come you are withdrawing large sums of money and you are unemployed?...Why are you using different names to claim your money?" (Participant 8HS).

Apart from the above-mentioned agents of the state apparatus, some respondents observed that cyber-criminals sometimes turn to the spiritual realm to help with their online criminal activities. Specifically, participant 16Y commented that some corrupt spiritualists prepare magic armlets for cyber-criminals in return for economic benefits:

"Some small boys weh dey come my shop here even say dem dey use juju take money from people hand for internet" [I heard from some young men, my customers here (referring to her shop), that they – cybercriminals, are using magic to defraud their victims]

B Peer Group

Also, some respondents felt that merely associating with delinquent peers could make a child more vulnerable to corruption in adulthood. This notion was vividly captured in Participant 5EB's statement:

"*A lot of the things children grew up with, they pick up from home, peers, friends, and the people they associate with. In Nigeria, when the parental upbringing is weak, children normally follow a bad convoy of peers, because in Nigeria there is constant drive to follow the wagon:* "if you can't beat them, you join them".

C University Environment

Other participants indicated that even when young people leave their homes to acquire a university education, they often become vulnerable to university-campus gang membership, the notion being that gang members are most likely to participate in cyber-fraud offences. This idea was captured below:

"*In Nigerian universities, there are different social classes and those on top are mostly cult members, 419 boys* [which have a bond in high social class] *because they have high financial capabilities.*
Lastly, whilst there is a link between gang-membership and cyber-fraud offences, some adult Nigerians seem to sympathize with cybercriminals. This is evident in a participant's 3CE observation:

"*If a 419 boy is arrested, people would be sympathetic to him. They would ask, what type of crime has he committed? Is it just because he defrauded someone? Is it bigger than the ones people in government are committing? Why are they treating the small boy [cybercriminal] as if he has done something terrible*?"

V. DISCUSSION

Three key findings emerged from the analyses. Firstly, "a good family environment" and a range of other family-related factors encourage 'high moral standards' in young people and also equip them to resist structural corruption in society. Secondly, Nigerian society appears to have more negative reactions toward traditional crime than toward cybercrime. Thirdly, some established cybercriminals in Nigerian universities are 'gang members' who have an external support-network comprised of people in positions of authority.

With respect to "a good family environment" and the range of family-related factors, interviewees frequently brought up the phrase 'moral standard' during their interviews. Some of them interchangeably referred to 'moral standards' as '*person wey no sabi wayo' or 'person wey no fit magomago*', which means a person who has a high moral standard or a person who would never cheat/scam others. While some of them linked it directly to a person's susceptibility to involvement in cyber-criminality, others identified it as being a crucial aspect of quality parenting in Nigeria.

This notion of 'moral standard' echoes Situational Action Theory (SAT) [30], [31], [32], [33], which postulated that regardless of a person's level of self-control, a high moral standard is necessary and sufficient to buffer them from becoming involved in criminal activities. The centrality of the family in instilling strong morality in people during childhood is critical: a person with a low level of morality is deemed most likely to cyber victimize others. Also, if people develop high moral standards during childhood, they would be more equipped to eschew corrupt practices in society. Arguably, a good family environment could be invaluable in protecting children and instilling resilience, autonomy and self-regulation against structural corruption. Also, the fact that most cybercrime breeding factors in Nigeria converge remarkably along the lines of familial variables reinforces a long-standing assertion in the Nigerian juvenile delinquency literature. According to this long-standing assertion, family-related

factors are the most important ones in terms of juveniles' risks for involvement in criminal activities [16], [17]. One possible explanation for this assertion is that family obligations are at the core of the Nigerian cultural values and societal expectations encourage these values in people.

Secondly, in Nigeria, there is less negative societal reaction against cybercrime than terrestrial crimes such as armed robbery. This socio-cultural 'understanding' could be due to the relative absence of 'real victims' and 'blood and knives' when it comes to cybercrime. This invokes Becker's [6] notion about the relativity of crime and deviance. Unlike the case of cybercrime, negative societal reactions against terrestrial crime could act as a deterrence mechanism even in the presence of low moral standards. Therefore, it is the society's reactions that define what is a 'crime' in Nigeria [4], [6]. Social reactions inherent in Nigeria, in terms of cybercrime may have knock-on-effects on of cybercrime involvement among the youths. This suggests that morality may be more of an index factor for 'cybercrimes' than terrestrial crimes in the Nigerian context. It also reinforces the importance of a complex web of familial factors and structural forces, alongside cultural forces, when it comes to explaining cybercrime involvement among Nigerian youth.

The implication is that the role of familial factors in the lives of the university students who are often the subject of cybercrime studies were taken for granted and not properly teased out, given assertions from a number of developmental theories about the stability of delinquency across the lifespan [9], [34]. One possible explanation for this oversight in samples of university students could be due to cross-sectional studies generally neglecting a long-time historical perspective on the complexity and diversity of lives within the target group.

Thirdly, consistent with the existing literature on cybercrimes in Nigeria [18], [19], [20], [25], data from this study revealed that agents of state apparatuses were thought to be promoting cyber fraud in Nigeria. According to interviewees, some corrupt politicians, police officers, bankers and spiritualists have unique relationships with cyber-criminals (locally known as yahoo boys). The relationships between these 'yahoo boys' and the authorities have reciprocal effects on both groups. Analysis of data on corruption revealed that during Nigerian elections, corrupt politicians have been known to hire unemployed youths and undergraduates known as '[4]*area boys'* to intimidate their political opponents. The implication is that the politicians who employ these 'thugs' during elections also protect them from being arrested – other criminal activities.

Analyses have also revealed that the relationship between university '*area-boys*' or 'thugs' and politicians is important for understanding the linkage between children and cybercrime in Nigeria. In Nigerian universities, the presence of 'thuggism' 'cyber-criminality' and 'cultism' are very visible. A majority of '*area boys*' in Nigerian universities are university cult members. As Tade [20] articulated, most cyber-criminals have been implicated in cultism and the use of "magic" to ensnare their victims. In fact, data from this current study revealed that, cybercriminals (*yahoo boys*), university 'thugs' (*area boys*), and university cult members (cult boys) are intertwined; they collectively sustain the highest level of social hierarchy within the Nigerian university context.

These groups of boys (*yahoo*, cult, and *area boys*) 'who are often up to no good' constitute the inner circles of Nigerian universities. Evidently, it accords with various findings that have identified Nigerian higher institutions as breeding grounds for cybercrime [18]. Therefore, in complementing the existing studies, this paper conceptualizes these groups of individuals as 'the circle of bad boys' (CBB). The CBB are the ruling class in Nigerian universities, due to their role in creating and discarding informal university rules. They have an unequal power relation with other university students: These three groups of CBB are strongly linked to one another, partly through their links with corrupt politicians, police officers, bankers and spiritualists in Nigeria society, and partly due to their role in sustaining the highest level of social hierarchy in Nigerian universities. The centrality of 'university' here is of the utmost importance, because university students generally serve as a source of aspiration to most Nigerian children. Most children look up to university students from their towns and villages as role models, and the CBB members therefore act as negative role models.

According to participant 2BM who claimed to be a cult member in his university days:

"*The beginning of cultism in Nigerian universities in those days was to fight against oppression, fight for people who were too weak to fight for themselves. But in recent years, [cult members] those who are suppose to fight against oppression now become the oppressors, intimidating their fellow students physically and financially with 419 benefits. Upon that, online fraudulent guys do not face the consequences of their crimes, because the big ogas [big bosses] in politics, police force, support them. This makes it attractive for their friends from good homes too. This group of people, online thieves, control things in the universities*".

This is consistent with the idea that cybercriminals intimidate other students. They also bring more bribery into the university system, even beyond the halls of academia [19]. In line with Ojedokun and Eraye [19], the analyses have found that in Nigerian universities, the conspicuous lifestyles of yahoo boys and the violent identities of cult/area boys cast their shadows on other students and create the social strata. As a result, they may

[4] Area boys, comprising mostly teenagers, are loosely organized street-level gangs in Nigeria.

condition "good guys, from good homes" to join them so as to be protected from psychosocial humiliation.

One possible implication of this phenomenon in Nigerian universities is that it makes CBB membership attractive for other students. It could erode the resistance to criminal activities in other students, especially those with the type of low self-control described in Gottfredson and Hirshchi's [35] general theory of crime, and in accordance with SAT [30], [31], [32], [33]. However, unlike the general theory of crime, wherein low self-control has a direct and causal link to all offending, with SAT, a person's capacity to exert self-control depends on the presence or absence of a strong moral standard.

This emphasizes the importance of familial factors in sustaining morality in children, even in the presence of negative peer influence and other external factors such as corruption. Given the primacy of family name and obligations in Nigerian society, the promotion of high moral standards during childhood could act as a viable micro-mechanism in combating cybercrime involvement in Nigeria. On the other hand, it suggests that Nigerian university students who were able to resist CBB membership have a very high level of both self-control and moral standards. Regarding cybercrimes in Nigeria, these types of individuals are not often represented in various discourses such as the media. In fact, they are not only under-represented or ignored, but their very existence is often denied.

This problem runs extremely deep. If the majority of police officers in Nigeria are not corrupt, it would be difficult for members of the public to bribe them. By the same token, if members of the public are not vulnerable to corrupt practices, it would be challenging for police officers to successfully initiate corrupt practices. Most corrupt individuals often use the saying "…if you can't beat them, you join them" to justify their actions; the saying in itself sustains corrupt practices and normalizes them in Nigeria to some extent. Also, it makes it challenging for the 'good apples in a rotten basket' to reinvent the 'wheel of the game' [36] in Nigerian policing. In other words, the alleged informal principles of Nigerian policing could render good officers in 'ground-level services' vulnerable to intentionally or unintentionally corrupt practices when dealing with members of the public who are powerful and corrupt.

The spiritualists in Nigeria may be conceptualised as individuals who are engaged in a form of public service. The role of spiritualism in cybercrime in Nigeria intersects with the notion of 'escapelessness' in the pre-colonial Sub-Saharan region [37]. Tankebe [37, pp.69] explained that "[E]scapelessness meant that the ancestral spirits were thought to be all-knowing; no violation of the norms of society and no offender escaped their surveillance". It could be that those who represent the ancestral spirits in the physical realm (i.e., priests) are not so immune to corruption as the ancestors in the spiritual sphere. It could that the priests' vulnerability to corrupt practices has metamorphised over time from the age-old customary gift-giving gestures in Nigeria. The key point is that whilst spiritualists in the physical sphere aid cyber-criminality in contemporary Nigeria, they 'policed' crime in pre-colonial Nigeria. Arguably, due to the fact that some spiritualists today are caught up in the web of bribery and corruption within cybercriminal networks, they promote cybercrime. In turn, they negatively impact on the maintenance of high moral standards in some children. This in turn could increase children's likelihood of involvement in the socioeconomic cybercrime and highlights Jaishankar's [38] idea of cyber criminology - that the causations of crimes that are relevant in the cyberspace concurrently impact in the physical space and vise versa.

VI. CONCLUSION

Contrary to most cybercrime data in Nigeria, this current paper has emphasized that a range of familial factors such as "a good family environment" have more influence on a person's susceptibility to involvement in cybercrime than external factors such as corruption. As well, peer pressure within the university environment and Nigerian society in general has an influence. Consequently, this paper has used insights from the moral standard element of SAT [30], [31], [32], [33] to shed light on the socioeconomic cybercrime in Nigeria. Specifically, these insights have helped to underscore the significance of familial factors when addressing cyber fraud involvement among Nigerian youths. Concomitantly, it stressed that importance of cyber criminology [38] because in terms of the causations of cybercrimes, the physical space and the digital space are intertwined.

The above findings should be interpreted with caution, as there were only 17 participants (a small sample). That said, unlike some other studies that have interviewed people who have openly identified themselves as cybercriminals, this paper has explored parents' perceptions on the causes of cybercrime in Nigeria. Moreover, these limitations by no means undermine the importance of this study's achievement: highlighting that a complex web of familial factors and structural forces, alongside cultural forces, explains the degree of cyber fraud involvement on the part of Nigerian youths.

ACKNOWLEDGMENT

MY PROFOUND GRATITUDE GOES TO MICHAEL RUSH, JUSTICE TANKEBE, AND THE ANONYMOUS PEER REVIEWERS FOR THEIR USEFUL COMMENTS. I AM GRATEFUL TO ALL MY INTERVIEWEES FOR THEIR PARTICIPATIONS . I THANK C. MONKS FOR PROOFREADING A VERSION OF THIS ARTICLE. I ALSO THANK THE FOLLOWING MEMBERS OF MY UNIVERSITY: J. CRAMPTON, G. PRICE, L. COLES-KEMP, L. CAVALLARO, K. MARTIN, FOR THEIR SUPPORT ON VARYING DEGREES. I AM ALSO GRATEFUL TO SIRKKA AND OLIVER FOR THEIR ADVICE. I THANK THE EPSRC AND THE UK GOVERNMENT AS PART OF THE CENTRE FOR DOCTORIAL TRANING IN CYBER SECURITY (CDT) AND THE INFORMATION SECURITY GROUP AT ROYAL HOLLOWAY, UNIVERSITY OF LONDON.

Reference List:

[1] "The world Factbook," 2001. [Online]. Available: https://www.cia.gov/library/publications/resources/the-world-factbook/geos/ni.html. Accessed: June. 01, 2016

[2] Adogame, A. 2007. [online] The 419 Code as Business Unusual: Youth and the Unfolding of the Advance Fee Fraud Online Discourse, *International Sociological Association e-bulletin,* available at: http://www.isa-sociology.org/publ/e-bulletin/E-bulletin_7.pdf, accessed July, 10, 2016.

[3] "Internet Crime Complaint Centre, 2010 [online]: *https://pdf.ic3.gov/2010_IC3Report.pdf*. Accessed May 09, 2015.

[4] S. Ibrahim, "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals," *International Journal of Law, Crime and Justice,* volume 47, pp. 44-57. DOI: *http://dx.doi.org/10.1016/j.ijlcj.2016.07.002. Dec. 2016.*

[5] Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. Cybercrime: Introduction, Motivation and Methods. In Cybercrime, Digital Forensics and Jurisdiction (pp. 3-23). Springer International Publishing.2015.

[6] Becker, H. *Outsiders: Studies in Sociology of Deviance.* New York: Simon and Schuster Ltd.1997.

[7] Farrington, D. Childhood risk factors for young adult offending: Onset and persistence. In Lösel, F., Bottoms, A. E. and Farrington, D. P. (Eds.) Young Adult Offenders: Lost in Transition? London: Routledge. 2012.

[8] D. P. FARRINGTON, D. JOLLIFFE, R. LOEBER, M. STOUTHAMER-LOEBER, and L. M. KALB, "The concentration of offenders in families, and family criminality in the prediction of boys' delinquency," *Journal of Adolescence*, vol. 24, no. 5, pp. 579–596, Oct. 2001.

[9] T. E. Moffitt, "Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy," *Psychological Review*, vol. 100, no. 4, pp. 674–701, 1993.

[10] J. H. Derzon, "The correspondence of family features with problem, aggressive, criminal, and violent behavior: A meta-analysis," *Journal of Experimental Criminology*, vol. 6, no. 3, pp. 263–292, Jun. 2010.

[11] J. Belsky and S. R. Jaffee, "The multiple determinants of parenting," in *Volume Three: Risk, Disorder, and Adaptation*. Wiley-Blackwell, 2015, pp. 38–85

[12] Ibrahim, S. A Binary Model of Broken Home: Parental Death-Divorce Hypothesis of Male Juvenile Delinquency in Nigeria and Ghana. *Contemporary Perspectives in Family Research.* ed. / Sampson Lee Blair; Sheila Royo Maxwell. (Vol. 9, pp. 311 - 340) New York: Emerald Publishing, 2015.

[13] B. Cole and A. Chipaca, "Juvenile delinquency in Angola," *Criminology and Criminal Justice*, vol. 14, no. 1, pp. 61–76, Sep. 2013.

[14] K. E. Boakye, "Correlates and predictors of juvenile delinquency in Ghana," *International Journal of Comparative and Applied Criminal Justice*, vol. 37, no. 4, pp. 257–278, Nov. 2013.

[15] O. N. I. EBBE, "Juvenile delinquency in Nigeria: The problem of application of western theories," *International Journal of Comparative and Applied Criminal Justice*, vol. 16, no. 1-2, pp. 353–370, Jan. 1992.

[16] Ugwuoke, C. U., & Duruji, O. U. Family Instability and Juvenile Delinquency in Nigeria: A Study of Owerri Municipality. *Journal Of Humanities And Social Science, vol. 20, non. 1, pp. 40-45.2015.*

[17] Sanni, K., Modo, F., Uduh, N., Ezeh, L. and Okediji, A. "Family types and juvenile delinquency issues among secondary school students in Akwa Ibom State, Nigeria: Counseling implications." *Journal of Social Science*, vol. 23, no. 1, pp. 21-28.2010.

[18] J. O. Aransiola and S. O. Asindemade, "Understanding Cybercrime perpetrators and the strategies they employ in Nigeria," *Cyberpsychology, Behavior, and Social Networking*, vol. 14, no. 12, pp. 759–763, Dec. 2011.

[19] Ojedokun, U. A., & Eraye, M. C. Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, vol. *6*, no.2, pp. 1001-1013.2012.

[20] O. Tade, "A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon," *Human Affairs*, vol. 23, no. 4, Jan. 2013.

[21] A. Kazdin, "Contributions of risk-factor research to developmental psychopathology," *Clinical Psychology Review*, vol. 17, no. 4, pp. 375–406, 1997.

[22] D. P. Farrington, "Cross-national comparative research on criminal careers, risk factors, crime and punishment," *European Journal of Criminology*, vol. 12, no. 4, pp. 386–399, Jul. 2015.

[23] [Online]. Available: http://TransparencyInternational (2014) 'The 2014 Corruption Perception Index', available at: http://www.transparency.org/cpi2014, accessed, 30/12/15. Accessed: Jul. 18, 2016.

[24] J. Odumesi, "Messaging Cyberforensics Standard for Cybercrime Investigations, *Advances in Multidisciplinary & Scientific Research, vol. 1, no.2.pp.141-146.2015.*

[25] Adeniran, A.I. Café culture and heresy of yahooboyism in Nigeria in K. Jaishankar (eds) Cyber Criminology: Exploring Internet Crimes & Criminal Behavior: New York: CRC Press. 2011.

[26] Code, L. What Can She Know?: Feminist Theory and the Construction of Knowledge. New York: Cornell University Press. 1991.

[27] G. W. Ryan and H. R. Bernard, "Techniques to identify themes," *Field Methods*, vol. 15, no. 1, pp. 85–109, Feb. 2003.

[28] O. C. Robinson, "Sampling in interview-based qualitative research: A theoretical and practical guide," *Qualitative Research in Psychology*, vol. 11, no. 1, pp. 25–41, Nov. 2013.

[29] Bryman, A. *Social research methods*. Oxford: Oxford university press. 2015.

[30] D.-H. HAAR and P.-O. H. WIKSTRÖM, "Crime propensity, criminogenic exposure and violent scenario responses: Testing situational action theory in regression and Rasch models," *European Journal of Applied Mathematics*, vol. 21, no. 4-5, pp. 307–323, Jun. 2010.

[31] Wikström, P. H. Crime propensity, criminogenic exposure and crime involvement in early to mid adolescence. Monatsschrift fur Kriminologie und Strafrechtsreform 92: 253–66. Wikström, Per-Olof H. 2010a Situational action theory. In Encyclopedia of Victimology and Crime Prevention, ed. Bonnie Fisher and Steven Lab. Thousand Oaks, CA: Sage. 2009.

[32] Wikström, P. H. Situational action theory. In Encyclopedia of Criminology and Criminal Justice, ed. Gerben J.N. Bruinsma and David Weisburd. New York: Springer. 2014.

[33] Wikström, P. H. *Why crime happens: A situational action theory*. In Analytical Sociology, ed. Gianluca Manzo. New York: Wiley. 2014.

[34] D. P. Farrington, "Childhood origins of antisocial behavior," *Clinical Psychology & Psychotherapy*, vol. 12, no. 3, pp. 177–190, 2005.

[35] Gottfredson, Michael R. and Travis Hirschi. *A General Theory of Crime*. Stanford, CA: Stanford University Press.1990.

[36] Reiner, R. *The Politics of the Police.* Oxford: Oxford University Press.

[37] J. Tankebe, "Colonialism, legitimation, and policing in Ghana," *International Journal of Law, Crime and Justice*, vol. 36, no. 1, pp. 67–84, Mar. 2008.

[38] Jaishankar, K. Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In: Jaishankar, K. (Ed.), *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii-xxxv). Boca Raton, FL, USA: CRC Press, Taylor and Francis Group. 2011.

.

VOLUME 19, ISSUE 2, PAGES 63–80 (2018)

Criminology, Criminal Justice, Law & Society

CRIMINOLOGY, CRIMINAL JUSTICE, LAW & SOCIETY

E-ISSN 2332-886X
Available online at
https://scholasticahq.com/criminology-criminal-justice-law-society/

Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists

Suleman Lazarus

Independent Researcher.

ABSTRACT AND ARTICLE INFORMATION

This study sets out to examine the ways Nigerian cyber-fraudsters (*Yahoo-Boys*) are represented in hip-hop music. The empirical basis of this article is lyrics from 18 hip-hop artists, which were subjected to a directed approach to qualitative content analysis and coded based on the moral disengagement mechanisms proposed by Bandura (1999). While results revealed that the ethics of *Yahoo-Boys*, as expressed by musicians, embody a range of moral disengagement mechanisms, they also shed light on the motives for the Nigerian cybercriminals' actions. Further analysis revealed additional findings: "glamorization/de-glamorization of cyber-fraud" and "sex-roles-and-cultures". Having operated within the constraint of what is currently available (a small sample size), this article has drawn attention to the notion that Yahoo-Boys and some musicians may be "birds of a feather." Secondly, it has exposed a "hunter-and-antelope-relationship" between Yahoo-Boys and their victims. Thirdly, it has also highlighted that some ethos of law-abiding citizens is central to Yahoo-Boys' moral enterprise. Yahoo-Boys, therefore, represent reflections of society. Arguably, given that Yahoo-Boys and singers are connected, and the oratory messages of singers may attract more followers than questioners, this study illuminates the cultural dimensions of cyber-fraud that emanate from Nigeria. In particular, insights from this study suggest that cyber-fraud researchers might look beyond traditional data sources (e.g., cyber-fraud statistics) for the empirical traces of "culture in action" that render fraudulently practices acceptable career paths for some Nigerian youths.

Article History:

Received 25 November 2017
Received in revised form 7 March 2018
Accepted 20 March 2018

Keywords:

youth culture and popular music, yahoo boys and cyber criminology, neutralization techniques, advance fee fraud and organised crime, moral disengagement mechanisms, glamorization of cybercrime, sex roles, victims of romance scam, cyberpsychology

© 20 18 *Criminology, Criminal Justice, Law & Society* and The Western Society of Criminology
Hosting by Scholastica. All rights reserved.

Corresponding author: Suleman Lazarus, CCCSR, 6 Thornes Office Park, Monckton Road, West Yorkshire, Wakefield, WF27AN, UK. Email: suleman.lazarus@gmail.com

Fraudster*: "Honey, your sparkle always lights up my heart."* Victim*: "Oh, hmmm, I love you, darling."* Fraudster*: "Me too. I can't wait to hold you in my arms. But there's a little problem."* Victim*: "What is it, honey?"* Fraudster*: "I urgently need a small amount of money to hasten the process of my travelling documents and visa."* Victim*: "How much do you need, darling?"* [1] The above type of dialogue may be commonplace in a cyber-fraud context, and we often hear stories about cyber-fraudsters duping victims through catfish[2] relationships (Whitaker, 2013). While we may know little about cyber-fraudsters (Levi, 2016), in recent years there has been an upsurge in victim-oriented studies (Button et al. 2014; Cross, 2016; Owen, Noble & Speed, 2017; Webster & Drew, 2017). At least two factors are responsible for this upsurge: first, the extensive media coverage of high-profile victims in the West (BBC, 2016), and second, victims are mainly defrauded in the context of "love" and "friendship" (Kopp et al. 2015; Whitty & Buchanan, 2016). Romance is in itself a source of excitement and mystery, whereas romance that is created through *freestyle tricks* is different. *Freestyle tricks* is the use of online dating sites and apps by cyber-fraudsters to befriend unsuspecting victims to the extent that victims fall in love with the perpetrators and support them instrumentally (Ibrahim, 2016a). Research on the psychology of cyber-fraudsters could offer a greater understanding of cyber-fraud, especially the fraud that emanates from Nigeria. According to the Federal Bureau of Investigation (FBI, 2010) statistics[3], Nigeria is the third worst country globally when it comes to the prevalence of "cybercrime" perpetrators.

The term "cybercrime" encompasses a broad spectrum of rule-breaking behaviours, such as cyber-fraud, cyber-bullying, cyber-stalking and cyber espionage (Hutchings and Chua, 2016; Yar, 2016). This research, however, focuses exclusively on cyber-fraud, not least because it constitutes the bulk of cybercrimes that emanate from Nigeria (Adeniran, 2011; Ojedokun & Eraye, 2012; Trend Micro & INTERPOL, 2017). The defrauding of victims for monetary benefits is the most significant theme in the analysis of Nigerian cybercriminals, and cyber-fraud, for this study, refers to the computer or/and internet-mediated acquisition of financial benefits by false pretence, impersonation, counterfeiting, forgery or any other fraudulent representation of facts (Ibrahim, 2016a). While there are many types of cyber-frauds associated with the broader canon (Button & Cross, 2017; Schoepfer et al. 2017), researchers have predominantly associated the Nigerian cybercriminals with Advance Fee Fraud (AFF) or "419" fraud (Igwe, 2007; Adogame, 2009; Rich, 2017). AFF is a confidence trick in which victims are deceived into advancing relatively small sums of money in the hope of realising a much larger gain (Chang, 2008; Rich, 2017). The term "419" is historically derived from section 419 of the Nigerian Criminal Code[4] and deals with fraud and money laundering. Therefore, this research acknowledges that, historically, online 419-fraud has been situated in a Nigerian context, and thus, "cybercrime" in this article is exclusively understood as cyber-fraud (e.g., romance-scam, advance fee fraud). Before the digitalization of these crimes, a Nigerian lawyer, Fred Ajudua, supposedly revolutionised multiple offline "419"-formats (Longe, Mbarika, Kourouma, Wada, & Isabalija, 2010). The online versions of 419 and AFF are locally known as "*yahoo-yahoo*" (Adeniran, 2011; Melvin & Ayotunde, 2010). "*Yahoo-yahoo*" is coined from the dominance of Yahoo emails, apps and instant messaging in perpetrator-victim communications during the mid-2000s (Trend Micro & INTERPOL, 2017) when there was an Internet boom in Nigeria. The perpetrators of "*yahoo-yahoo*" are popularly called "*Yahoo-Boys*" (Aransiola & Asindemade, 2011). Having defined the above terms, this article examines the ways *Yahoo-Boys* are represented in hip-hop music. In particular, it assesses the connections between them (*Yahoo-Boys* and musicians) looking for, in Swidler's (1990) term, the empirical clues of "culture in action."

Media Representations of Yahoo-Boys and Singers Connections

"*In the Nigerian music industry, Yahoo boys reign supreme*" - Music Critic, Tayo

D'banj's song "*Mobolowowon*," which came out in 2004, was the first song with a cyber-fraud-theme in hip-hop music (Tayo, 2017). It supposedly described how the singer escaped from the British police when he was wanted for credit card scams in London. Beyond *D'banj's* alleged biographical accounts, he explained in a recent interview[5] that "most of the new generation record labels are founded by Yahoo-Boys" (e.g., Daily Post, 2018). *D'banj's* explanation aligns with some Nigerian music critics and commentators' assertions that "Yahoo-Boys have floated music labels, and some are singers themselves" (e.g., Tayo, 2017, p.1). Such speculations have drawn huge (social) media attention. They have, for example, triggered various discussions on national TV channels in Nigeria, such as "Linda Ikeja Hot Topics TV Show" (2017). While

one might still question whether singers and Yahoo-Boys are indeed "birds of a feather that flock together," it is worth considering the following: First, according to the Daily Post (2017), many singers do not only benefit directly from the cyber-fraud, but they are also ex-con men (see also University of Wisconsin-Madison, 2017). For example, "9ice," a singer with a cloak of respectability, mentioned "street-names" of some five popular Yahoo-Boys, allegedly his associates, in his recent song "Living Things" (Punch, 2017a). Like "*9ice*," other singers (DJ Sidez featuring Slimecase and Masta T) also mentioned names of well-known Yahoo-Boys in their recent song, "Oshozondi[6]. However, not all singers share a similar viewpoint (Computer World, 2010). Microsoft and the Nigerian government have jointly sponsored some singers to campaign against Yahoo-Boys as part of a war against cyber-fraud in Nigeria. In particular, Microsoft's Internet Safety Security and Privacy Initiative for Nigeria was prompted by one primary reason: to reduce the impact of Yahoo-Boys on singers and vice versa. Second, beyond the above loose link between Yahoo-Boys and singers, Nigerian hip-hop star Dammy Krane was arrested on cyber-fraud charges before boarding a private jet in Miami (Neal, 2017). Additionally, while *Sauce Kid*, a Nigerian rapper, was jailed in America for cyber-fraud (Punch, 2017b), another prominent figure in the Nigerian music industry, *Special Ed*, had been arrested in the USA for First Degree Forgery (Information Nigeria, 2014). Third, apart from these direct connections between cyber-fraud and singers, *Rapper N6* (a singer), summarised his views on the connection between Yahoo-Boys and musicians as follows:

> Entertainers cannot be separated from illegal money....Most of the highest money that they've [singers] made come from people that have made money from illegal means....The new guys are the militants [Yahoo-Boys]. They are the new money guys. We are all trying to get a militant godfather. (as cited in Hot TV Topics, 2017, p.1)

Insights from the above suggest that Yahoo-Boys and music artists may not be two separate entities with clearly defined boundaries. Beyond the realm of social media, however, research has not yet established the connections between Yahoo-Boys and musicians. In other words, apart from media speculations (Punch, 2017a, 2017b), the ethics of Yahoo-Boys and their representation in music have only been discussed as gossip in most Nigerian chatroom forums and some television channels. For this article, the ethics of Yahoo-Boys can be understood as a set of perceptual alterations that offer them "psychological shields" to justify their conduct and thus, circumvent self-condemnation (Bandura, 1999; Sykes & Matza, 1957). Three questions are at the core of this study: [1] What are the ethics of Nigerian cyber-criminals as expressed by music artists? [2] Which techniques do artists deploy to describe their views on cyber-criminals? [3] What might the justifications say about the motives for "cybercrime"? To gain a deeper insight into the ways crime and illegal money are represented in hip-hop music in general, this article proceeds with a literature review. Doing so is prompted by two central drives: [1] to examine the core characteristics of hip-hop culture and [2] to assess the main features of Yahoo-Boys.

Literature

Hip-Hop Ethics and Culture

"Keep in mind when brothas start flexing the verbal skillz, it always reflects what's going on politically, socially, and economically[7]"

Most generalizable research on hip-hop has traced the genesis of hip-hop in Nigeria to African communities in the South Bronx (New York), where contemporary hip-hop music originated during the 1970s (Blanchard, 1999; Shonekan, 2013). However, Bailey (2014) and Persaud (2011) pointed out that hip-hop culture is rooted in multiple cultures, and prominent among these are West African cultures. Hip-hop singers were historically believed to serve as "*griots*" in their social communities. Since the *griots* were respected West African oral historians and praise-singers (Keyes, 2002; Persaud, 2011), they were believed to have preternatural creative and emotional intelligence or talents (Blanchard, 1999). For Schulz (1997) and Blanchard (1999), the oratory messages of *griots* generally attract more followers than questioners. The "*griots*" have immense power to impose reception, not primarily due to the uniqueness of their messages, but also because their messages have always been at the heart and lips of the masses – they represent the harsh realities of their lives (Blanchard, 1999; Schulz, 1997). In this context, the *griots* are the voices of those who otherwise have no power to impose reception. For Bourdieu (1977), powerful speakers speak, not exclusively to be understood, but more importantly, to be believed, respected, and repeated (p. 648). Repeating discourses normalizes their claims, and the orthodoxy of the *griots* by implication is almost certain.

The American hip-hop and rap[8] artists, through their African oral storytelling heritage, could be seen

as the contemporary *griots*, and by the same token, they are powerful speakers who have an immense power to impose reception (Blanchard, 1999; Keyes, 2002; Persaud, 2011). These music artists not only depict and reflect the realities of American inner cities (Royster, 2016), but they primarily embody street entrepreneurship, practices, dispositions, and habits. This type of embodiment has been referred to as "street habitus" (Ilan, 2015, p.57; see also Dimou, 2017). By implication, most American artists, through songs, performances and records, chant about their life stories and experiences such as gang violence, glamorization of wealth, illicit drug business, street hustling, and thug life (Dimou, 2017). For example, the following song from Notorious B.I.G, "Juicy," (Genius Lyrics, 2018, p.1) summarised a part of his life succinctly. "*Yea, this album is dedicated to all the teachers that told me I'd never amount to nothing, to all the people that lived above the buildings that I was hustling in front of that called the police on me when I was just trying to make some money to feed my daughter*" (Genius Lyrics, 2018, p.1). Therefore, it is key to remember that first, hip-hop singers such as Notorious B.I.G are like the *griots* (Peraud, 2011), and their songs can influence attitudes possibly due to the artistic and emotional framing of their messages (Louw, 2017). Second, a specific aspect of hip-hop singers' dispositions and attitudes is street habitus, and as Ilan (2015) noted, street habitus is fundamentally embodied and cannot be easily "tried on" (p. 57).

Hip-hop music symbolizes street habitus and contributes to who we are: "In short, hip-hop lyrics instruct listeners in how to make sense of urban street crime and how to understand the identities of those who participate in crime (or avoid) it" (Kubrin, 2005, p.367). Kubrin's (2005) study on music and behaviour pointed out that while hip-hop and rap music do not cause crime, they offer vivid vocabularies of motive, which justify criminal conduct and provide a way for listeners to understand and appreciate them. Rehn and Sköld (2003) noted that the effects on listeners of narratives that glamorise material goods, such as in Puff Daddy and colleagues' hit song "[I]t's All About the Benjamins" ("*Lex and Range Rovers…/...../It's All About the Benjamins, baby...*"), is plausible. *Benjamin* here denotes the US$100 note, because it has Benjamin Franklin's head on it. Such songs may influence listeners' attitudes toward the consumption of brand goods and the means to obtain them (via crime or otherwise).

Like their historical antecedents in America, researchers have argued that Nigerian songs such as "I go chop your dollar" were supposedly produced for the recruitment of youths into cyber criminality and "easy ways to affluence" (e.g., Oduro-Frimpong, 2014). In the Nigerian context, due to the absence of an economic, medical, and social security system as well as political impunity (Shonekan, 2013; Smith, 2008), hip-hop music has served as an escape vehicle to self-employment for some Nigerian youths (Oladipo, 2017; Shonekan, 2013). Most university students "hustle" to pay school fees, and they face unemployment or poor wages and inefficient health care when they graduate (Ibrahim, 2016a; Smith, 2017). As a consequence, established Yahoo-Boys are often perceived as heroes and transnational "Robin Hoods" who take "dollars" from the rich in the West and give to the poor in West Africa (Tabu, 2011). Indeed, according to some media commentators, "many awesome Yahoo-Boys and kind-hearted artists are using their money to open foundational programs and help the poor masses" (e.g., Segun, 2017, as cited in Naijaloaded, 2017, p.1). Although the links between unemployment/poverty and offending rates are far from straightforward (Newburn, 2016), it is plausible that economic hardship unified the destiny of hip-hoppers and that of Yahoo-Boys in part, offering real-life scripts for singers to represent "street entrepreneurship" and cyber-fraudsters in their songs. This study will henceforth provide a brief historical overview on Yahoo-Boys.

Yahoo-Boys and University Students/Graduates

Historically, the colonial[9] police and head teachers had noted that Nigerian schoolboys were "excellent psychologists" in manipulations (e.g., U.S. Consulate, 1949). These teenagers were described as "psychologists" because they defrauded many "knowledgeable and intelligent" victims in Western societies with postal scam letters (Ellis, 2016, p.28). These observations illuminate the psychology of the offline fraudsters. Some researchers have shed light on the psychology of their online successors (i.e., cyber-fraudsters) by examining their fraudulent emails (purportedly from Yahoo-Boys; Adogame, 2009; Dion, 2010; Rich, 2017). These researchers highlighted that authors[10] of scam emails (who may or may not be Nigerians) deploy a "trust rhetoric" (Rich, 2017), embody a "Machiavellian worldview" (Dion, 2010) and use "authoritative and urgent" language (Chang, 2008) to defraud their victims. In particular, Rich (2017) investigated how fraudsters invoke trust with the Nigerian-email-scam-formats and how recipients interpret such trust-laden offers. He found that references to trust language are most common in emails purported to have originated from the African continent and those that promised a large amount of money. These studies (Chang, 2008; Dion, 2010; Rich, 2017) expanded our understanding of the

psychology behind the scam letter format. The current study builds on insights from the above studies, and it examines the cultural dynamics of cyber-fraud. Indeed, it investigates the ways Yahoo-Boys are represented in hip-hop music, and the connections between them (Yahoo-Boys and musicians) searching for, in Swidler's (1990) term, the empirical traces of "culture in action."

Decoding the term Yahoo-Boys is a critical entry point for understanding the cultural dynamics of cyber-fraud originating in Nigeria. The "Boys" after the term "Yahoo" suggests that the perpetrators of the infamous sweetheart swindles, among other types of AFF, may be primarily male. In support, there is a reasonably clear pattern to suggest that young adult male Nigerians, mainly university students/graduates, constitute the bulk of cyber-fraudsters (Aransiola & Asindemade, 2011; Tade & Aliyu, 2011). While the accusation of male university students may be reminiscent of that of the colonial schoolboys in the 1940s mentioned above, the evidence on the demography of contemporary Nigerian swindlers demands a closer look. For example, Aghatise (2006) speculated that "80% of perpetrators in Nigeria are students in various Higher Institutions" (p. 2). However, he failed to provide any evidence for his claim. Empirical evidence for the prominence of male university students in the theatre of cyber-fraud came from Aransiola and Asindemade (2011), Tade (2013), Ojedokum and Eraye (2012) and Tade and Aliyu (2011). Like Ojedokum and Eraye (2012) and Tade and Aliyu (2011), Aransiola and Asindemade (2011) specifically contended that [1] male university students between the ages of 22-29 years mainly commit cyber-fraud that originates from Nigeria; [2] Nigerian universities serve "as the breeding grounds" for "*yahoo-yahoo*" (p. 762); [3] some 'Yahoo-boys' subscribe to the occult-economy[11], that being the use of spiritual-powers in the virtual world for wealth generation.

However, while the above studies portrayed youth cultures and male juvenile offenders to assume the appearance of ever-increasing outrage in Nigeria, they solely relied on university students as their samples, and this pattern of data has led to the authors' assertions. Conversely, other researchers who interviewed students and non-students (Jegede, Elegbeleye, Olowookere, & Olorunyomi, 2016), parents (Ibrahim, 2016b), and students and spiritualists (Melvin & Ayotunde, 2010) arrived at the same conclusion as the above authors (e.g. Aransiola & Asindemade, 2011). Considering that cyber-fraud involves cyberspace, this social phenomenon should not be limited by parochial conceptions that give it little or no global significance in our computer age (Hall, 2013 Levi, 2016; Kirillova, Kurbanov, Svechnikova, Zul'fugarzade, & Zenin, 2017). Indeed, the virtual world and cultural nuances in society are not separate entities (Jaishankar, 2011; Ibrahim, 2016a; Stratton, Powell and Cameron, 2017). These studies (e.g., Jegede et al., 2016; Ojedokum & Eraye, 2012), therefore, provide clues on the dynamics of youth cultures and cyber-fraud. Most Nigerian youths, despite economic hardship and the glamorization of crime, do resist criminal activities, whereas, for other youths, cyber-fraud constitutes innovative self-employment (Adogame, 2009; Jegede et al., 2016). The key point is that offenders and non-offenders respond differently to the same social and contextual conditions in society. "The line dividing good and evil cuts through the heart of every human being"[12], whereas there is no objective viewpoint for the rationalization of an "immoral" act (Bandura, 1999).

Theoretical Guidance

Unlike in a Nigerian context, Hutchings (2013) and George (2014), in Western societies, have used "neutralization techniques" (Sykes & Matza, 1957) and the "moral disengagement mechanisms" (Bandura, 1999) theories to assess cybercrime respectively. The neutralization techniques proposed by Sykes and Matza (1957) and moral disengagement mechanisms put forward by Bandura (1999) are essentially based on the premise that offenders and non-offenders have the same normative orientations and general moral beliefs (Ribeaud & Eisner, 2010). Similar to Sykes and Matza's (1957) argument that individuals offend if they find excuses to remove the feelings of blame from themselves, Bandura, Barbaranelli, Caprara, and Pastorelli (1996) argued that "people do not ordinarily engage in reprehensible conduct until they have justified to themselves the rightness of their actions" (p. 365). There is considerable overlap between the neutralization techniques and Bandura's (1999) mechanisms of moral disengagement (summarised in Table 1, modified from Ribeaud & Eisner, 2010). Since people do not ordinarily offend until they have justified to themselves the rightness of their actions (Bandura, 1999), it is conceivable that this theoretical background will shed light on the cultural dynamics of cyber-fraud that originates from Nigeria.

Table 1: Conceptual Similarities Between Theories

Cognitive Mechanism	Neutralization Techniques (Sykes & Matza, 1957)	Moral Disengagement (Bandura, 1999; Bandura et al., 1996)
Cognitive Restructuration	1. Appeal to Higher Loyalties 2. Euphemistic labeling (implied)	1. Moral Justification 2. Euphemistic Labeling 3. Advantageous Comparison
Minimizing Own Agency	Denial of Responsibility	1. Displacement of Responsibility 2. Diffusion of Responsibility
Disregarding/Distorting Negative Impact	Denial of Injury	1. Disregarding Consequences 2. Distorting Consequences
Blaming/Dehumanizing Victim	Denial of Victim	3. Attribution of Blame 3. Dehumanization
Condemnation of Condemner	Condemnation of Condemner	

Note: Table modified from Ribeaud and Eisner, 2010, p. 301

Method

Lyrics Data Collection

The following systematic steps listed were taken to select lyrics listed in Table 2:

1. Searched on Google with phrases such as "list of Nigerian musicians" and made a list of all Nigerian Hip-hop and rap artists.
2. Validated list with two professional Nigerian hip-hop DJs to ascertain that no artists have been missed. The underlying idea is that while some singers are famous in the realm of public spaces such as dance halls, they might not have produced their official first album. For example, *2Face Dibia* (one of the most successful Nigerian pop stars) was already a national star while performing in Nigerian university-campuses before he released his first album.
3. Visited the online profiles of each singer found and selected the ten most popular songs in descending order of significance from each artist. The criterion that songs are relatively the most popular of each artist ensured that the music had reached a significant proportion of the population as is evident in the case of '*Yahooze*[13]'
4. Selected only songs produced in English, pidgin English, and three major indigenous languages in Nigeria (Igbo, Yoruba, and Hausa) respectively. Nigeria has over 500 indigenous languages, and due to practical reasons, songs produced in other numerous ethnic languages were excluded.
5. Selected songs produced between 2007 to 2017 because while Nigerian hip-hop emerged in the late 1980s, it has only become highly commercialized and accessible during the internet boom in the late 2000s (Adjirakor, 2017; Inyabri, 2016; Shonekan, 2016). The availability of electronic music production, editing, and distributing applications facilitated open participation in the street-entrepreneurship of hip pop music for underprivileged youths (Shonekan, 2016). Like Kubrin's (2005) study, which investigated rap music in the USA from 1992 to 2000 for a related reason, our study chose to capture this period.
6. Read the lyrics of the remaining songs from music websites such as "freenaijalyrics.com" and "sweetlyrics.com" while searching for cyber-fraud themes.
7. Made a list of songs that explicitly depicted "yahoo-yahoo" while using a wide spectrum of Yahoo-Boys' slangs such as "maga," "wire wire," "419," "Gameboy," "freestyling," and so on as a guide.
8. Validated the list with four professional DJs in Lagos and Abuja (the previous and current capital cities respectively) from the four popular nightclubs concerning the popularity of selected songs in leisure spaces. A list of songs was presented to these DJs, and any song that was not

endorsed by at least two DJs was excluded. Any song with less than 50% (n=2) of these DJ was excluded.

9. Selected 18 songs that explicitly represented 'Yahoo-Boys' over the period of 10 years as outlined in Table 2 (i.e., 2007-2017 and nine songs for every five years).
10. Songs were selected in descending order of significance; that is, if a singer has two songs that depicted cybercrime, the one that most explicitly represented 'Yahoo-Boys' ethics was chosen in place of the other one. Except if a singer is not a lead singer and has one or more co-singers involved in a second song, only one song from each singer is eligible for inclusion in order to have, in Kubrin's (2005) term, a diverse collection of lyrical "vocabularies of motive."
11. Lyrics were subjected to a directed approach to qualitative content analysis (DAQCA) (Hsieh and Shannon, 2005), and coded based on the moral disengagement mechanisms proposed by Bandura (1999). Findings, as shown in Table 3, are discussed.

Table 2: List of Songs Studied

Song
1. Yahooze (from Olu Maintain, 2008)
2. Living things (from 9ice, 2017)
3. Maga don pay (from Kings, 2015)
4. Yahoo boyz (from X-busta, 2016)
5. Yahoo boys (from Prince Hollywood, 2009)
6. Yahoo boys (from Gnext, 2011)
7. Maga don pay (from Larry Prince, 2013)
8. Maga don pay (from Kelly Handsome, 2008)
9. Maga no need pay (from Banky W and other artists, 2010)
10. I go chop your dollar (from Nken Owoh, 2010)
11. 419 state of mind (from Modenine, 2011)
12. I dey block IP (from Tupengo, 2011)
13. 2musssh (from Reminisce, 2013)
14. Irapada 2:0 (from Junior Boy featuring 9ice, 2016)
15. Maga don pay (from Jupitar featuring Patorinking, 2016)
16. Penalty lyric (from Small Doctor, 2017)
17. Mercies of the lord (from Oritse Femi, 2008)
18. Maga don pay (from Big Joe, 2015)

Table 3: Theory and Themes in Songs Connection

Cognitive Mechanism	Neutralization Techniques (Sykes & Matza, 1957)	Moral Disengagement (Bandura, 1999; Bandura et al., 1996)	Songs and Themes (songs as chronologically listed in Table 2)
Cognitive Restructuration	3. Appeal to Higher Loyalties 4. Euphemistic labeling (implied)	4. Moral Justification 5. Euphemistic Labeling 6. Advantageous Comparison	1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 18
Minimizing Own Agency	Denial of Responsibility	3. Displacement of Responsibility 4. Diffusion of Responsibility	1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18

Blaming/Dehumanizing Victim	Denial of Victim	3. Attribution of Blame 3. Dehumanization	1, 3, 4, 5, 6, 7, 8, 10, 11, 15, 16, 18

Discussion

Four central themes emerged from lyric data[14]. Three of them support the theoretical framework outlined in Table 3, whereas a new theme also emerged. Accordingly, the following fundamental themes are most basic to the discussion that follows: [1] blaming/dehumanizing the victim, [2] minimizing own agency, [3] cognitive restructuration, and [4] glamorization and de-glamorization of cyber-fraud.

Blaming/Dehumanizing the Victim

Firstly, as represented in most of the lyrics assessed, Yahoo-Boys blame victims for bringing suffering on themselves. Specifically, according to singers such as Modenine*, "some call it 419 or advance fee fraud /I say it's getting doe* [money] *from greedy victims."* For Yahoo-Boys, victims are "greedy," and hence, they are to be blamed for their plight. Conversely, the attribution of blame to victims enables Yahoo-Boys to circumvent the feeling of guilt for their fraudulent actions. "Mistreatment that is not clothed in righteousness makes the perpetrator, rather than the victims, blameworthy" (Banduras, 1999, p.203). Yahoo-Boys do not only blame victims, but they also dehumanize them. It is simplistic to suggest that Yahoo-Boys dehumanize their victims fundamentally because of the distance between them (facilitated by networked computers). At some stage of the romance scam cycle, the Yahoo-Boys' "freestyle format" may involve face-to-face interactions (Ibrahim, 2016a). In a similar vein, Whitty and Buchanan's (2016) interview study indicated that victims of romance scams actually meet their sweetheart swindlers offline. Arguably, irrespective of the distance between the victims and the perpetrators, as Wang and Krumhuber (2016) reminded us, objectification becomes permissible when targets are seen as senseless or foolish, hence being equated to mindless objects.

Accordingly, Yahoo-Boys commonly perceive victims as having low mental abilities, and likened them to stupid sub-humans. For example, as expressed in the lyrics, Yahoo-Boys used derogatory names for victims, particularly, "*maga*" or/and "*mugu*," which locally connote(s) "foolish, senseless, and gullible." However, linguistically, both words have slightly different meanings, where "*maga*" is more derogatory than "*mugu*," and means "foolish, stupid, or senseless animal." The mechanisms of moral disengagements, such as de-humanization, precede immoral acts and are central to their immediate causation (Bandura, 1999). The utilization of "*maga*" and "*mugu*" in "*yahoo-yahoo*" primarily functions as a "shield" against feelings of guilt. While the use of "*maga*" and "*mugu*" offers significant insights into dehumanization within cyber-fraud and Yahoo-Boys' ethics, this study will briefly introduce some critical Nigerian cultural folklore so as to contextualize these explanations.

In Nigeria, hunters commonly consider themselves wiser than and superior to the animals they hunt, which are conceived of as foolish and inferior. The antelope is the most common game-beast, generally thought to symbolize the rewards of the hunt. By the same token, hunters are believed to possess superior mental acumen in comparison with antelopes, which often fall into their traps (Igwe, 2007). It is the perception of mental superiority that enables hunters to bypass the feeling of guilt for killing senseless sub-humans (antelopes). As linguist Igwe (2007) noted, Nigerian fraudsters generally thought of their victims as "*mgbada*" (antelope in Igbo language), and of themselves, in contrast, as hunters in the digital realm. By implication, hunting is a "game." A game in itself is not a crime. In the same vein, when cyber-scam is likened to hunting, it becomes a game. This is vividly captured in Larry Prince's song: "*Maga don pay* [the senseless animal has paid]*, it's a holiday for the Gameboys../.../....*" Metaphor establishes the basis of people's everyday comprehension of life (Santa Ana, 2002). In hunting, victims are divested of human characteristics, and if perpetrators believe "yahoo-yahoo" is a game, it is a game in terms of its consequences. "It is difficult to mistreat a humanized person without suffering personal distress and self-condemnation" (Bandura, 1999, p. 200). Relatedly, the dehumanization of victims in the personification of hunter and antelope is a crucial entry point to unpack the code word "*maga*" (victims). Based on the above insights and Igwe's (2007) analysis of "*mgbada*," this article concedes that the word "*maga*" has linguistically metamorphosed from "*mgbada*" (antelope).

The Igbo-speaking communities in the Delta and Anambra states of Nigeria are essential for understanding fraud neologism and vocabulary (from *mgbada* to *maga*). Although the actual demography of cyber-fraudsters and their offline antecedents is not fully established, Longe and colleagues' (2010) assumptions offer a glimpse of the main players. According to these authors, some high profile graduate fraudsters, such as Fred Ajedua (who originated from these Igbo speaking regions), dominated the 419-game before the "cyber" component of fraud emerged in Nigeria. It is reasonable, therefore, to theorise that the indigenous

language used by these high-profile, educated fraudsters has facilitated the entry of "*mgbada*" into the "419" vocabulary. The deployment of this coined word (from *mgbada* to *maga*) is particularly significant as it sheds light on the ethics of the Yahoo-Boys, as depicted in most of the songs studied. The perpetrator-victim relationship as that of a hunter and his game-animals (prey) is based on dehumanization: the ethics of the Yahoo-Boys. The centrality of the dehumanization of victims is vividly captured in the following lyric by Nkem Owoh: "*/You be the mugu,..../When they fall into my trap o /I dey show them fire.../...*" (You are the foolish,…./ when they fall into my trap, I show them no mercy).

Minimizing Own Agency

A second theme found in the lyrics examined in this study was the obscuring or minimization of the agentive role of the Yahoo-Boys concerning the harms they cause by shifting responsibility to circumstances beyond their control, such as poverty and unemployment. As expressed by a majority of music artists in this study, mass unemployment, abject poverty, and a lack of social welfare in Nigeria are responsible for the *"yahoo-yahoo"* that originates from Nigeria. Some singers are beneficiaries of active Yahoo-Boys' fraudulent activities (University of Wisconsin-Madison, 2017), while some others are convicted cyber-fraudsters or ex-cyber criminals (Neal, 2017; Punch, 2017b) as mentioned. It is reasonable, therefore, to suggest that the rationalization of cyber-fraud as found in most songs in Table 2 exposes the displacement and diffusion of responsibility as a key moral disengagement technique deployed by Yahoo-Boys. By implication, both Yahoo-Boys and the singers externalize the locus of control for socially sanctioned behaviours. The sympathetic representation of Yahoo-Boys and their "self-employment" endeavours online in the hip-hop songs examined are hinged on the assumption that harsh socio-economic realities in Nigeria are fundamentally a push factor. This type of representation also supports Ibrahim's (2016a, p.55) thesis that 'what constitutes cybercrime in Nigeria is rooted in socio-economics.'

However, not all Nigerian youths resort to Internet fraud as an answer to economic insecurity. Arguably, by obscuring the agentive role behind their harmful cyber actions, Yahoo-Boys not only justify their reprehensive activities but also remove feelings of blame from themselves. Self-exemption from the consequences of cyber-fraud is one of the moral disengagement mechanisms (Bandura, 1999) or neutralization techniques (Skyes & Matza, 1957) that delinquents deployed to deny responsibility for their harmful actions. The following lyric from X-Busta captures this strategy: "*... no job for street/no pay, no way, how boys go eat? /.../Dem no go do yahoo if dem get choice/....*" (no employment, no income, no hope, how will the youths survive? They would not commit internet fraud if they had the choice). According to this excerpt from X-Busta's song, most Nigerian youths face acute unemployment or poor wages, and "*yahoo-yahoo*" has become a way of survival for them. Closely related to the minimization of agency is cognitive restructuration.

Cognitive Restructuration

The song lyrics analysed also indicated that cognitive restructuring is one of the moral disengagement mechanisms the Yahoo-Boys use to make their cyber criminality appear acceptable. The following lines from G-Next's song, "*next of kin/bank to bank/ attorney fee/ affidavit/ cost of transfer*/….", as well as Prince Hollywood's song, "*Wilson has paid attorney fees, Wilson has paid the cost of transfer/…. Affidavits…/*", are a clear illustration of the deployment of euphemistic language as a means of cognitive restructuration. Yahoo-Boys use professional legal and banking terms, as represented in the above songs, to mask their criminal acts with a cloak of respectability. Whilst the "attorney fees" and "affidavits" scamming format are traceable to 419-letter scams prior to the digital version, the deployment of such terms in cyber-fraud illustrates the contemporaneity and efficacy of these old scam templates or formats.

Scam templates enable Yahoo-Boys to sanitize their fraudulent actions: "Cognitive restructuring of harmful conduct through sanitizing language, and exonerating comparisons, taken together, is the most powerful set of psychological mechanisms for disengaging moral control" (Bandura, 1999, p.196). Yahoo-Boys also use advantageous comparisons to render condemnable benevolent or righteous actions. The following lyrics by X-Busta are instructive in this regard: "*/Police pursue thiefs/ Leave Yahoo boyz o/ Police pursue thiefs/ Leave Yahoo boyz o/...Dem no wan carry gun so dem grab computer/ as dem no see job after dem fight for Aluta/...*" (Police go after thieves, leave Yahoo-Boys alone... They [Yahoo-Boys] have refused to carry guns [commit violent crimes], instead, they have only used computers [commit cyber-fraud], because of the lack of jobs after a university education). Similarly, Modenine's song is an example too: "…advance fee fraud/ [is] getting doe [money] from greedy victims abroad/Without pulling a trigger contact or slashing with a sword…"

These lines of the song make a sharp contrast between "*thieves*" and Yahoo-Boys. Culturally, the actions of "thieves" including non-violent ones, such

as pickpocketing in public spaces, often receive vigilante justice (Smith, 2008, 2017). On the other hand, multiple variations of crimes committed through deception, such as the embezzlement of public funds, are perceived as "business as usual" in a Nigerian context (Smith, 2008, 2017). Indeed, they are "business" in terms of their consequences. Insights from Chawki, Darwish, Khan, and Tyagi (2015) suggest that Nigerian cyber-fraudsters and hard-working, law-abiding citizens share a similar overarching ethos: the philosophy that "knowledge is power." So, possibly, this similarity may be implicated in shaping people's perceptions/attitudes towards Yahoo-Boys in relation to "thieves." There is no objective viewpoint for the critique or compliment of an "immoral" act (Becker, 1967/1997; Garson, 2015; Reiner, 2016). The process by which an action is graded as a crime in relation to other actions is a "moral enterprise" (Becker, 1967/1997, p. 9). The moral enterprise here encompasses not only the worldviews of Yahoo-Boys and their allies (hip-hoppers) but also involves the socio-cultural views of Nigerian society. The moral sanctification of Yahoo-Boys' actions as opposed to that of "thieves" normalizes their claims in Nigeria. Nigerian society is, therefore, the moral entrepreneur in the social construction of "*thieves*" and "Yahoo-Boys": "While terms appear to be objective, they are actually underpinned by value judgements that are rooted in particular cultural assumptions" (Ribbens, McCarthy, & Edwards, 2011, p. 6). The sharp comparison used by Yahoo-Boys to avoid self-condemnation, therefore, is grounded in a Nigerian contextual situation and the cultural meaning of "thieves" in relation to Yahoo-Boys. The Nigerian hip-hop songs examined here, therefore, are reflective of social realities in Nigeria, like their historical antecedents in America. Closely related to the above is the concept of "drift" (Matza, 1967), which intertwines with the Yahoo-Boys' cognitive restructuration.

Criminals are generally attracted to delinquency, not because of oppositional morality, but because of an exaggerated adherence to widely held "subterranean" values, such as the pursuit of adventure, hedonic lifestyles, excitement, and leisure activities (Matza, 1967; Matza & Sykes, 1961). For Matza (1967), delinquents transiently flirt with both convention and crime, responding in turn to the demands of each. Comparably, our data analysis suggests that Yahoo-Boys transiently flirt with both internet fraud and convention, which is evident in the following lyrics. While the first one, by Olu Maintain (2008), illustrates that Yahoo-Boys work hard in the same way that law-abiding citizens work weekdays and have leisure time during the weekends, the second one, by X-Busta, makes a moral justification in an attempt to redeem their condemnable cyber actions: [1] *"Monday, Tuesday, Wednesday, Thursday, Boys dey hustle / Friday, Saturday and Sunday gbogbo aye, Hennesy, Champagne, Mowet, for everyone/.../"* (Weekdays, boys are busy on the Internet, weekends, they shut down clubs, declaring champagne and expensive spirits for everyone). [2] *"/this one na self employment/so dem go see food for their table/ attend to family issues, so life go stable/"* (this is self-employment, so as to put food on the table, take care of family needs, so as to maintain a stable family).

Despite the small sample size of this study, the above verses can be seen as a window into the Yahoo-Boys' world. Yahoo-Boys view "hard-work" and having a stable family as virtuous, whereas, paradoxically, victims of cyber-fraud (and their families) may experience severe negative psychological and financial consequences (Kopp et al. 2015; Whitty & Buchanan, 2016). Irrespective of victims' predicaments, Yahoo-Boys achieve paradoxical adaptations through cognitive restructuration (Bandura, 1999). Additionally, given that they do not oppose conventional values (e.g., the virtues of hard-work), it is reasonable to suggest that they are attracted to "*yahoo-yahoo*" due to their exaggerated adherence to the pursuit of adventure and hedonic lifestyles (as vividly captured in Olu Maintain's lyrics above). Arguably, the Yahoo-Boys' perspectives on "hard-work" (directly or by implication) overlap with the ethos of law-abiding citizens in many respects. The above comparison is reminiscent of Matza's (1967) idea that offenders may not stand as an alien in the body of society, but may represent a disturbing reflection instead. The moral compasses of the two seemingly separate camps (offenders and non-offenders) appear to have a high degree of congruence. Also, the theory that most Nigerians glamorize wealth irrespective of its source (through crime or otherwise; e.g., Adeniran, 2011) reinforces the view that the boundary between offenders and non-offenders is blurred, inasmuch as the people involved in such moral categorization are economically successful and "hard-working." Also, given that musicians are generally influential as the "griots," by implication, they may shape the perceptions of cyber-fraud in the eyes of music lovers.

Glamorization and De-Glamorization of Cyber-Fraud

Unlike the themes discussed above, the "glamorization and de-glamorization theme" did not fit squarely with the overlapping theoretical frameworks in Table 1 because they cannot be termed as neutralization techniques as such.

Nonetheless, they are also revealing. Whilst most songs (*n*=16) explicitly glamorised the Yahoo-Boys, only one directly de-glamorised them. For example, Kelly Handsome's song explicitly glamorised cyber-fraud: *"...Maga don pay/ Mugu don pay / shout hallelujah.../...hallelujah hallelujah owo.../ .../...hallelujah hallelujah ego.../... hallelujah hallelujah kudi, kudi../I don suffer, but I now don hammer, papa God don bless me, no one can change it.../..."* (The gullible has paid, the senseless has remitted/ shout hallelujah…/...hallelujah hallelujah money…/...hallelujah hallelujah money…./…/ hallelujah hallelujah money, money… I have suffered a lot, but now I have hit the jackpot, Almighty God has blessed me, [and] no one can change it). While the above song glamorized cyber-fraud, it embodied biblical allusion (i.e. a reference to the Bible regarding prosperity as a critical element of religiosity). It reflects Yahoo-Boys' worldview that 'earthly riches' have spiritual aetiology mentioned earlier. The notion of spirituality in wealth acquisition (occult-economy) as depicted in Kelly Handsome's song, therefore, is also an aspect of the glamorization of cyber-fraud.

However, seven artists who collectively composed/performed the de-glamorised song, "*Maga no need pay*," were allegedly sponsored by Microsoft and the Nigerian government (Computer World, 2010). As far as this research is concerned, the song itself remains the only song that has been put forward against "*yahoo-yahoo*" in Nigeria (Computer World, 2010). By implication its content is not only dislocated from dominant narratives, but as "9ice" pointed out, it is "out of touch with reality" (Punch, 2017a, p.1) because "fraud is the way the less privileged people take care of these family in Nigeria" (Punch, 2017b, p.2). Capturing Nigerian socio-economic reality, Oritse Femi's song mostly blames harsh economic situation and bad government for Yahoo-boys' actions, which implicitly supports the glamorization narratives: "…*Bad government leading my people astray / Some working everyday but their salary dem no dey pay* [salary is not enough]." The critical point is that the oratory narratives of singers who glamorized Yahoo-Boys reflected the socio-economic realities of Nigerian situation more than the de-glamorization narrative: "*But maga no need pay to get a good degree/ or have a good opportunity*" (But victims do not need to make payment for the perpetrators to acquire a good degree/ or have a good job opportunity). For Barker and Taylor (2007) and Duncan (2017, p.33) "authenticity of an artistic creation" has both a representational element (something which is what it claims to be) and a cultural component (something which is in line with a contextual or cultural tradition). Based on the above definition, it is conceivable that the song "Maga no need pay" dislocates from the socio-economic and contextual conditions in Nigerian society in two central areas: representational and cultural.

Sex Roles and Cultures

Closely related to the glamorization of *yahoo-yahoo* is the idea that cyber-crime is male-dominated in a Nigerian context. Notably, like the male domination of cyber-criminality, the singers of all songs selected in Table 2 are male apart from song number nine: "Maga no need pay," which involved seven multiple artists. Allied with the above is the evidence for the prominence of young male Nigerians in the theatre of cyber-fraud mentioned (e.g., Jegede et al., 2016; Ojedokum & Eraye, 2012). In Nigerian society, the value of economic power (through crime or otherwise) is intertwined with the social work that it does (or fails to do) in human relationships (Smith, 2017). Insights from a range of gender-oriented studies about Nigeria (Chinwuba, 2015; Lazarus, Rush, Dibiana, & Monks, 2017) are revealing. Firstly, recent years have witnessed an upsurge of women in the paid workforce (Eboiyehi, Muoghalu, & Bankole, 2016), whereas 'men rather than women in this context, are predominantly socialized to be breadwinners' and the supreme head of the household (Ibrahim, 2015, p.329). Secondly, unlike women, economic power for men has limitless advantages. For example, a Nigerian man who has economic power, irrespective of his age, 'under customary and Islamic types of marriages can marry multiple wives' (Lazarus, Rush, Dibiana & Monks 2017, p.352). While he can even marry wives as young as 14 or 13 years old, depending on his "tastes" (Lazarus, Rush, Dibiana & Monks, 2017), culturally, even his adultery is seen as "a heroic feat" (Chinwuba, 2015; Smith, 2017). These types of gender relations not only shape the manner in which Nigerian society socializes its female citizens, but it also influences how women (and girls) are culturally expected to relate to males regarding wealth acquisition and status sustenance (Agozino, 2017; Mama, 1995). "Life online is an extension of life offline" (Morahan-Martin, 2000, p. 689), and as Ibrahim (2016a) speculated, "men's cultural positionality in society influences them to be generally more 'desperate' to achieve financial success than women online" (p. 54). Given that men are culturally and predominantly raised to be breadwinners illuminates the evidence for the male domination of cyber-fraud perpetrations and perhaps the prominence of male singers in Table 2.

Financial Incentives

Closely related to the gender dynamics of this type of cyber-fraud is the idea that 'financial incentives' are central to the meaning of 'cybercrime' in a Nigerian context. In fact, all the songs studied made explicit references to money, which translates as "*ego*," *"owo*," and *"kudi*" in the Igbo, Yoruba, and Hausa languages respectively (the three main indigenous languages in Nigeria). The centrality of money as expressed in these songs support the convergence of emerging evidence (Adogame, 2009; Jegede et al., 2016; Ojedokun & Eraye, 2012) that Yahoo-Boys are principally motivated by the need for economic reward and empowerment. The following lyrics from Prince Hollywood and Kelly Handsome, respectively, vividly captured this claim: [1] "*Hello Mr. Wilson / Yeah hello/how are you? I'm fine / have you made the payment? / yes, I've / Let me have the ten-digit number/2657785232 /.../ I'll get back to you as soon as possible / bye /...".* [2]*"Plenty, plenty maga, no matter the time you get the control numbers"* (multitude of senseless victims, no matter what time is it, you are sure to receive the payment numbers). Therefore, it is reasonable to conclude that pecuniary benefits in a Nigerian context mainly propelled cybercrime because the efficacy of a Yahoo-Boy is reflected in the number of victims that "*wire wire* [transfer money]" to him on a regular basis. For example, financial incentives are apparent in Kelly Handsome's song: *"/..plenty dollar straight to aboki make eh start to dey change it/...."* (plenty dollar straight to a bureau de change man [locally called aboki] to change it into naira [currently, $1 =380 naira]). Additionally, the crucial importance of money in *yahoo-yahoo* is also evident in most YouTube videos of songs in Table 2 (e.g., displaying briefcases filled with US dollars, spraying of dollar bills, showcasing expensive cars, partying with exotic drinks and women). In the language of Olu Maintain, which is reminiscent of Puff Daddy and colleagues' 1997 popular song (It's all about benjamins), "*it's all about 'Benjamin' baby/...*". Arguably, monetary success is a specific aspect of Yahoo-Boys*'* moral enterprise as represented by all songs investigated in this study.

Conclusion

This study has drawn attention to the notion that Yahoo-Boys and some musicians may be reciprocally constructing the destiny of one another. It is not only the first study to assess the ethics of Yahoo-Boys as expressed by music artists in a Nigerian context in particular, but it also the first study to explore how cyber-fraud, in general, is depicted in Nigerian popular music. Additionally, it has explored the presence of the mechanisms of moral disengagement (Bandura, 1999) and neutralization techniques (Sykes & Matza, 1957) in *yahoo-yahoo*. Thus, these analyses have not only helped to shed light on motives for cyber-fraud, but they have helped to conclude that Yahoo-Boys embody a range of the most powerful set of psychological mechanisms for disengaging moral control. Accordingly, given that Yahoo-Boys have been implicated in defrauding a multitude of victims all over the world (e.g., see Chang, 2008; Rich, 2017), insights from this study could provide a greater understanding about cyber-fraud that emanates from Nigeria.

Furthermore, the presence of the conceptual frameworks (see Table 1) in music lyrics illustrates the relevance and contemporaneity of these theories in modern times, and this is revealing. Hip-hop lyrics, therefore, could serve as useful tools in teaching these theories (see Table 1), because music not only may appeal more to a wide spectrum of students than abstract theories, but also musicians are more impactful and meaningful in the lives of youths than theorists (and abstract concepts). Additionally, the oratory messages of hip-hop singers may attract more followers than questioners, especially young people, as Inyabri (2016) noted. The lyrical words of musicians are often believed, respected, and repeated possibly as their historical antecedents, the *griots*. Repeating discourses normalize their claims. Hip-hop songs that legitimise *yahoo-yahoo* by implication could make it attractive to more people than otherwise. The adherents of music, in general, may not merely consume songs, but they may also co-produce the meaning they embody and thus, normalize the lyrical messages with all its entireties. Arguably, while music has the power to influence our beliefs and practices (Louw, 2017), online/offline, music contributes to making us who we are due to its artistic and emotional embodiment. Accordingly, this article has highlighted Jaishankar's (2011), Ibrahim's (2016a) and Stratton, Powell and Cameron's (2017) concept that contextual factors that are critical in the cyberspace are also vital in the physical space (implicating multiple academic disciplines). In exploring youth cultures, deviance, language, and communications, it has brought together topics of criminology, cultural sociology, social psychology, even musicology (if disciplinary boundaries are stretched a bit) to achieve its aims in an 'eclectic-way'[15]. It has done so by using data from a significant and underrepresented area (sub-Saharan hip-hop music).

Having operated within the constraint of what is currently available (a small sample size), this study's findings have limited generalizability at best. However, alongside the above contributions, it has not only underscored that some ethos of law-abiding

citizens is central to Yahoo-Boys' moral enterprise, but it has also highlighted that Yahoo-Boys, as represented in the hip-hop music examined, represent a disturbing reflection of our digital-age society. It is therefore critical that Yahoo-Boys phenomenon should not be ghettoized within parochial conceptions with little or no global significance. There is indeed a danger of failing to capture globalization in all of its complexities if each of such relevant social phenomenon is not taken as unconditionally serious beyond its physical geographical context (Hall, 2013; Tankebe et al. 2014). While this article has particularly examined Yahoo-Boys' phenomenon and their representation in hip-hop music within Nigerian society, by implication, these issues are also universalizable. Studies on rap music in the USA (e.g., Kubrin, 2005) have already enlightened cultural dimensions of street-violence and "thug life" because rap music could provide a way for listeners to understand and appreciate inner cities' youth culture and violence. Similarly, given that Yahoo-Boys and singers are "birds of a feather," and the oratory messages of singers may attract more followers than questioners, this study illuminates the cultural dimensions of cyber-fraud that emanate from Nigeria. In particular, insights from this study suggest that cyber-fraud researchers might look beyond traditional data sources (e.g., cyber-fraud statistics) for the empirical traces of "culture in action" (Swidler, 1990) that render fraudulent practices acceptable career paths for some Nigerian youths. Finally, further research may interview hip-hop singers to expand upon this study.

References

Adeniran, A.I. (2011). Café culture and heresy of yahooboyism in Nigeria. In K. Jaishankar (Ed.) *Cyber criminology: Exploring internet crimes & criminal behaviour*. New York, NY: CRC Press.

Adjirakor, N. D. (2017). Constructing the African city through hip-hop in" Nai Ni Ya Who?" by Muthoni the Drummer Queen. *Research in African Literatures*, *48*(1), 116–134. doi:10.2979/reseafrilite.48.1.08.

Adogame, A. (2009). The 419 code as business unusual: Youth and the unfolding of the advance fee fraud online discourse. *Asian Journal of Social Science*, *37*(4), 551–573. doi**:**10.1163/156853109X460192

Aghatise, E. J. (2006). Cybercrime definition. Retrieved from Computer Crime Research Center website: http://www.crime-research.org/articles/joseph06/2

Agozino, B. (2017). Critical perspectives on deviance and social control in rural Africa. *African Journal of Criminology and Justice Studies: AJCJS*, *10*(1), I.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 759–763. doi: https://doi.org/10.1089/cyber.2010.0307.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, *3*(3), 193–209. doi:10.1207/s15327957pspr0303_3

Bandura, A., Barbaranelli, C., Caprara, G. V., & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. *Journal of Personality and Social Psychology*, *71*(2), 364-374. doi:10.1037//0022-3514.71.2.364

Bailey, J. (2014). *Philosophy and hip-hop: Ruminations on postmodern cultural form*. Basingstoke, UK: Springer.

Barker, H., & Taylor, Y. (2007). *Faking it: The quest for authenticity in popular music*. New York, NY: WW Norton & Company.

BBC. (2016). I went to Nigeria to meet the man who scammed me. Retrieved from http://www.bbc.co.uk/news/world-africa-37632259

Becker, H. (1967/1997). *Outsiders: Studies in sociology of deviance.* New York, NY: Simon and Schuster.

Blanchard, B. (1999). The social significance of rap & hip-hop culture. Retrieved from Ethics of Development in a Global Environment (EDGE) website: http://web.stanford.edu/class/e297c/poverty_prejudice/mediarace/socialsignificance.htm

Button, M., and Cross, C. (2017). *Cyber Frauds, Scams and Their Victims*. New York: Taylor & Francis.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand journal of criminology*, *47*(3), 391-408.

Bourdieu, P. (1977). The economics of linguistic exchanges. *Social Science Information*, *16*(6), 645–668. doi:10.1177/053901847701600601

Chang, J. J. (2008). An analysis of advance fee fraud on the internet. *Journal of Financial Crime*, *15*(1), 71–81. doi:10.1108/13590790810841716

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). 419 scam: An evaluation of cybercrime and criminal code in Nigeria. In Chawki M., Darwish A., Khan M.A., Tyagi S (ed.) *Cybercrime, digital forensics and jurisdiction* (pp. 129–144). Berlin: Springer International Publishing.

Chinwuba, N. N. (2015). Human identity: Child rights and the legal framework for marriage in Nigeria. *Marriage & Family Review*, *51*(4), 305–336. doi:10.1080/01494929.2014.938286

Computer World. (2010). Nigeria uses celebrity to stem cybercrime. Retrieved from https://d321cxw853vaeo.cloudfront.net/article/335168/nigeria_uses_celebrity_power_stem_cybercrime/

Cross, C. (2016). Using financial intelligence to target online fraud victimization: Applying a tertiary prevention perspective. *Criminal Justice Studies*, *29*(2), 125–142. doi:10.1080/1478601x.2016.1170278

Daily Post. (2017). 9ice reacts to Falz' condemnation of his song allegedly glorifying 'Yahoo' boys. Retrieved from http://dailypost.ng/2017/06/23/9ice-reacts-falz-condemnation-song-allegedly-glorifying-yahoo-boys/

Daily Post. (2018). Most of the new generation record labels are founded by Yahoo boys' - D'banj. Retrieved from http://dailypost.ng/2018/03/01/nigerian-record-labels-owned-yahoo-boys-dbanj/, accessed 02/03/2018

Davies, E. E., & Bentahila, A. (2008). Translation and code switching in the lyrics of bilingual popular songs. *The Translator*, *14*(2), 247–272. doi:10.1080/13556509.2008.10799258

Dimou, E. (2017). Friendship, love and hip hop: An ethnography of African American men in psychiatric custody. *The British Journal of Criminology*, Volume 58, Issue 3, (6) 760–763. https://doi.org/10.1093/bjc/azx038

Dion, M. (2010). Advance fee fraud letters as Machiavellian/Narcissistic narratives. *International Journal of Cyber Criminology*, *4*(1/2), 630.

Duncan, D. (2017). Australian singer, American features: Performing authenticity in country music. *Language & Communication*, *52*, 31–44. doi:10.1016/j.langcom.2016.08.004

Eboiyehi, F. A., Muoghalu, C. O., & Bankole, A. O. (2016). In their husbands' shoes: Feminism and political economy of women breadwinners in Ile-Ife, Southwestern Nigeria. *Journal of International Women's Studies*, *17*(4), 102–121. doi:10.4314/afrrev.v5i3.67340

Ellis, S. (2016). *This present darkness: A history of Nigerian organized crime*. Oxford, England: Oxford University Press.

Federal Bureau of Investigation. (2010). Internet Crime Complaint Centre. Retrieved from https://pdf.ic3.gov/2010_IC3Report.pdf.

Garson, G. D. (2015). *Explaining Human Behavior: Social & Organizational Theories*. Asheboro, NC: Statistical Associates Publishers.

Genius Lyrics (2018) 'The Notorious B.I.G. – Juicy Lyrics'. Retrieved from https://genius.com/The-notorious-big-juicy-lyrics.

George, R. J. (2014). *Moral disengagement: An exploratory study of predictive factors for digital aggression and cyberbullying*. (Unpublished doctoral dissertation). Denton, TX: University of North Texas.

Gritsenko, E., & Aleshinskaya, E. (2016). Translation of song lyrics as structure-related expressive device. *Procedia-Social and Behavioral Sciences*, *231*, 165–172. doi:10.1016/j.sbspro.2016.09.087

Hall, T. (2013). Geographies of the illicit: Globalization and organized crime. *Progress in Human Geography*, *37*(3), 366–385. doi:10.1177/0309132512460906

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288. doi:10.1177/1049732305276687

Hot TV Topics. (2017). Linda Ikeja's Hot TV. Retrieved from https://www.lindaikejisblog.com/2017/7/you-cant-separate-entertainment-from-illegal-money-most-of-the-highest-money-entertainers-make-is-from-people-with-illegal-money-rapper-n6-says.html

Hutchings, A. (2013). Hacking and fraud: Qualitative analysis of online offending and victimization. In K. Jaishankar and Natti Ronel (Eds.) *Global*

criminology: Crime and victimization in the globalized era (pp. 93–114). Boca Raton, FL: CRC Press.

Hutchings, A & Chua, Y. (2016). Gendering cybercrime in T. J. Holt (ed.), *Cybercrime through an Interdisciplinary Lens* (pp. 167-188). Oxon: Routledge.

Ibrahim, S. (2015). A Binary Model of Broken Home: Parental Death-Divorce Hypothesis of Male Juvenile Delinquency in Nigeria and Ghana, in S. R. Maxwell and S. L. Blair (ed.) Contemporary Perspectives in Family Research, Volume 9, (pp.311-340) New York: Emerald Group Publishing Limited.

Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. doi:10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *Cybercrime and Computer Forensic (ICCCF), IEEE International Conference on* (pp. 1-9). IEEE. doi:10.1109/ICCCF.2016.7740439

Information Nigeria. (2014). Special ED Arrested. Retrieved from http://www.informationng.com/2014/05/mugshot-reveals-that-davidos-hypeman-special-ed-was-arrested-for-fraud-in-2011.html

Igwe, C. N. (2007). *Taking back Nigeria from 419: What to do about the worldwide e-mail scam--advance-fee fraud*. New York, NY: iUniverse.

Ilan, J. (2015). *Understanding street culture: Poverty, crime, youth and cool*. London, UK: Palgrave Macmillan.

Inyabri, I. T. (2016). Youth and linguistic stylization in Naija afro Hip hop. *Sociolinguistic Studies*, *10*(1/2), 89-108. doi:10.1558/sols.v10i1-2.27931

Jaishankar, K. (2011). Introduction: Expanding cyber criminology with an avant-garde anthology. In K. Jaishankar (Ed.), *Cyber criminology: Exploring Internet crimes and criminal behavior* (pp. xxvii-xxxv). Boca Raton, FL: CRC Press.

Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I., & Olorunyomi, B. R. (2016). Gendered alternative to cyber fraud participation: an assessment of technological driven crime in Lagos State, Nigeria. *Gender and Behaviour*, *14*(3), 7672–7692.

Keyes, C. L. (2002). *Rap music and street consciousness*. Chicago, Illinois: University of Illinois Press.

Kirillova, E. A., Kurbanov, R. A., Svechnikova, N. V., Zul'fugarzade, T. E. D., & Zenin, S. S. (2017). Problems of fighting crimes on the Internet. *Journal of Advanced Research in Law and Economics*, *8*(3), 849–856.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology*, *9*(2), 205-217.

Kubrin, C. E. (2005). Gangstas, thugs, and hustlas: Identity and the code of the street in rap music. *Social Problems*, *52*(3), 360–378. doi:10.1525/sp.2005.52.3.360

Lazarus, S. I., Rush, M., Dibiana, E. T. & Monks, C. P. (2017). Gendered penalties of divorce on remarriage in Nigeria: A qualitative study. *Journal of Comparative Family Studies*, *48*(3), 351–366.

Levi, M. (2016). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3–20. doi:10.1007/s10611-016-9645-3

Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., & Isabalija, R. (2010). Seeing beyond the surface, understanding and tracking fraudulent cyber activities. *International Journal of Computer Science and Information Security*, *6*(3), 124–135. Retrieved from https://arxiv.org/abs/1001.1993

Louw, P. E. (2017). Afrikaner Music and Identity Politics in Post-Apartheid South Africa. In U. Onyebadi (Ed.), *Music as a Platform for Political Communication* (pp. 89–108). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1986-7.ch005

Mama, A. (1995). Feminism or femocracy? State feminism and democratisation in Nigeria. *Africa Development*, *20*(1), 37–58.

Matza, D. (1967). *Delinquency and drift*. London, England: Transaction Publishers.

Matza, D., & Sykes, G. M. (1961). Juvenile delinquency and subterranean values. *American Sociological Review*, *26*, 712–19. doi:10.2307/2090200

Melvin, A. O., & Ayotunde, T. (2010). Spirituality in cybercrime (Yahoo Yahoo) activities among

youths in South West Nigeria in Elza Dunkels, Gun-Marie Franberg, & Camilla Hallgren (ed.), *Youth Culture and Net Culture: Online Social Practices* (pp. 357–376). Hershey, PA: IGI Global.

Morahan-Martin, J. (2000). Women and the internet: Promise and perils. *CyberPsychology & Behavior*, *3*(5), 683-691. doi:10.1089/10949310050191683

Naijaloaded (2017) 'AS E DEY HOT!! Segun Wire Blasts Falz For Saying Musicians Should Stop Hailing Fraudsters'. Retrieved from http://www.naijaloaded.com.ng/entertainment/e-dey-hot-segun-wire-blasts-falz-saying-musicians-stop-hailing-fraudsters, accessed 7/7/17.

Neal. D. J. (2017). Nigerian pop music star Dammy Krane arrested on fraud charges. *Miami Herald*. Retrieved from http://www.miamiherald.com/news/local/community/miami-dade/miami-gardens/article157185574.html

Newburn, T. (2016) Social disadvantage: Crime and punishment. In H. Dean & L. Platt (Eds.), *Social advantage and disadvantage* (pp.322–40). Oxford, England: Oxford University Press.

Oduro-Frimpong, J. (2014). Sakawa rituals and cyber-fraud in Ghanaian popular video movies. *African Studies Review*, *57*(2), 131–147. doi:10.1017/asr.2014.51

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Oladipo, O. T. (2017). Mirroring the message of some Nigerian hip-hop music. In A. Ojo, K. Traore, & O. Longe (Eds.), *Africans and globalization: Linguistic, literary, and technological contents and discontents* (pp. 93–98). Lanham, MD: Lexington Books.

Owen, T., Noble, W., & Speed, F. C. (2017). The Challenges Posed by Scammers to Online Support Groups: The 'Deserving'and the 'Undeserving'Victims of Scams. In *New Perspectives on Cybercrime* (pp. 213-240). London: Palgrave Macmillan.

Persaud, E. J. (2011). The signature of hip hop: A sociological perspective. *International Journal of Criminology and Sociological Theory*, *4*(1), 626–647. Retrieved from https://ijcst.journals.yorku.ca/index.php/ijcst/article/view/32157/29376

Punch. (2017a). Controversy as Falz tell singers to stop praising 'Yahoo boys.' Retrieved from http://punchng.com/controversy-as-falz-tells-singers-to-stop-praising-yahoo-boys/

Punch. (2017b). Nigerian rapper, Sauce Kid jailed in America. Retrieved from http://punchng.com/nigerian-rapper-sauce-kid-gets-two-year-jail-in-america-for-stealing-15388/

Rehn, A., & Sköld, D. (2003). All about the Benjamins–hardcore rap, conspicuous consumption and the place of bragging in economic language. CMS Conference. Retrieved from https://www.mngt.waikato.ac.nz/ejrot/cmsconference/2003/proceedings/organization/rehn.pdf

Reiner, R. (2016). *Crime, the mystery of the common-sense concept*. New York, NY: John Wiley & Sons.

Rich, T. (2017). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*(1), 208-225. doi:10.1057/s41284-017-0095-0

Ribbens McCarthy, J., & Edwards, R. (2011). *Key concepts in family studies*. London, England: Sage Publications.

Ribeaud, D., & Eisner, M. (2010). Are moral disengagement, neutralization techniques, and self-serving cognitive distortions the same? Developing a unified scale of moral neutralization of aggression. *International Journal of Conflict and Violence (IJCV)*, *4*(2), 298–315.

Royster, D. M. (2016). [Review of the book *Philosophy and hip-hop: Ruminations on postmodern cultural form* by J. Bailey]. *Journal of Hip Hop Studies*, *3*(1), 115-117.

Santa Ana, O. (2002). *Brown tide rising: Metaphors of Latinos in contemporary American public discourse*. Austin, TX: University of Texas Press.

Schulz, D. (1997). Praise without enchantment: Griots, broadcast media, and the politics of tradition in Mali. *Africa Today*, 44 (4), 443-464.

Schoepfer, A., Baglivio, M., and Schwartz, J. (2017). Juvenile Hybrid White-Collar Delinquency: An Empirical Examination of Various Frauds. *Criminology, Criminal Justice Law and Society*, 18 (2), 21-38.

Shonekan, S. (2013). The blueprint: The gift and the curse of American hip hop culture for Nigeria's millennial youth. *Journal of Pan African Studies*, *6*(3), 181–199.

Smith, D. J. (2008). *A culture of corruption: Everyday deception and popular discontent in Nigeria*. Princeton, NJ: Princeton University Press.

Smith, D. J. (2017). *To be a man is not a one-day job: Masculinity, money, and intimacy in Nigeria*. Chicago, IL: University of Chicago Press.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'?. International Journal For Crime, Justice And Social Democracy, 6(2), 17-33.

Swidler, A. (1990). Culture in action: Symbols and strategies. *American Sociological Review*, *51*(2), 273–286. doi:10.2307/2095521

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670. doi:10.2307/2089195

Tabu, H. (2011) Culture: Yahoo Boys – Nigerian scammers are just like us. Retrieved from https://goodmenproject.com/culture/culture-the-yahoo-boys-nigerias-scammers-arent-so-different-after-all/

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, *23*(4), 689-705.

Tade, O., & Aliyu, I. (2011). Social organization of Internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860–875.

Tankebe, J., Hills, A., & Cole, B. (2014). Emerging issues of crime and criminal justice in sub-Saharan Africa. *Criminology & Criminal Justice*, *14*(1), 3-7.

Tayo, A. O. (2017). How Internet fraud has taken over Nigerian music. Retrieved from http://www.pulse.ng/gist/9ice-falz-how-internet-fraud-has-taken-over-nigerian-music-id6886970.html

Trend Micro and INTERPOL (2017). Cybercrime in West Africa: Poised for an underground market. Retrieved from https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf

University of Wisconsin-Madison. (2017). Hybridity in West African popular culture. Retrieved from http://africa.wisc.edu/hybrid/2009/07/07/419-scam-nigerian-hip-hop/

US Consulate. (1949). Records of the US consulate, Lagos, Nigeria 1940-63: NARA ii, RG 84, box 1, C. Porter Kuykendall, consul-general, to Secretary of State, 16 May, 1949.

Wang, X., & Krumhuber, E. G. (2017). The love of money results in objectification. *British Journal of Social Psychology*, *56*(2), 354–372. doi:10.1111/bjso.12158

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF) Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, *19*(1), 39–53. doi:10.1177/1461355716681810

Whitaker, R. (2013). Proto-spam: Spanish prisoners and confidence games. *The Appendix*, *1*(4). Retrieved from http://theappendix.net/issues/2013/10/proto-spam-spanish-prisoners-and-confidence-games

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176–194. doi:10.1177/1748895815603773

Yar, M. (2017). Online Crime in Henry Pontell (ed.) *Oxford research encyclopedia of criminology: Criminology & Criminal Justice, Oxford: Oxford University Press*.

About the Author

Suleman Ibrahim Lazarus, educated in the United Kingdom (e.g. Lambeth College, University of Greenwich, London School of Economics and Political Science) is an emerging scholar particularly interested in: [a] the occult economy and organised crime; [b] masculinity, cybercrime, and hip-hop music; [c] 'troubling families', and feminist epistemologies of crime. His recent publications include: [a] 'Causes of Socio-economic Cybercrime in Nigeria', [b] 'Social and Contextual Taxonomy of Cybercrime: Socioeconomic theory of Nigerian cybercriminals', [c] 'Troubling Chastisement: A Comparative Historical Analysis of Child Punishment in Ghana and Ireland'.

Acknowledgments

My gratitude goes to Professor Tim Newburn (London School of Economics & Political Science), Dr Nandini Dasgupta (University of Greenwich) and Dr Justice Tankebe (University of Cambridge), for their thoughtful comments on parts of my initial draft. I thank the three anonymous reviewers and the editors of CCJLS for their insightful recommendations. I also thank Mr Edward Tochukwu Dibiana, for his useful comments on the trilingual lyrics translations, and the 'DJs' for validating the songs in this study. I am also grateful to Dr Stephen Wyatt and Dr Kate Johnston-Ataata for proofreading portions of my draft.

Endnotes

[1] An excerpt from an online chatroom app.

[2] A relationship that is forged by one side through adopting a fraudulent or fictional online persona.

[3] However, critical perspectives pointed out that the statistics the FBI relied on to inform the currency of cybercrime perpetrators across nations are socially and selectively constructed. By implication, the FBI's claims are merely pictorial representations of that construction [https://doi.org/10.1016/j.ijlcj.2016.07.002]

[4] Nigerian Criminal Code Act: [http://lawsofnigeria.placng.org/laws/C38.pdf]

[5] D'banj was interviewed at the Social Media Week, Nigeria, February 28, 2018.

[6] Oshozondi was released in 2018: [https://itunes.apple.com/gb/album/oshozondi-feat-slimcase-masta-t-single/1337331237]

[7] Davey D. (1998) "Why Is Rap So Powerful". *Davey D's Hip-Hop Corner.* [http://www.daveyd.com/whyrapispowerart.html]

[8] 'Rap is a branch of hip-hop music, which makes use of rhyme, rhythmic speech, and street vernacular, which is recited or loosely chanted over a musical soundtrack' (Keyes, 2002, p.1).

[9] Nigeria was created by the British government through colonization from 1914 to 1960 (Lazarus et al., 2017).

[10] Authors of scam emails may or may not be Nigerians, and "there is an impossibility of knowing if every cyber-criminal using the Nigerian 419 or AFF letter/email templates is actually a Nigerian citizen" (Ibrahim, 2016a, p.51).

[11] The occult economy refers to the idea that the spirit world is an actual source of wealth and as a result, real or imagined, of magical means, can be used for material ends.

[12] A quote from a Russian historian, Aleksandr Solzhenitsyn [https://www.goodreads.com/author/quotes/10420.Aleksandr_Solzhenitsyn]

[13] Ex-US Secretary of State Colin Powell has joined a Nigerian performer, Olu Maintain on stage, while he sang his hit Yahooze [http://news.bbc.co.uk/1/hi/entertainment/7670788.stm]

[14] Given that most of the songs are bilingual, and not in standard English, as Davies and Bentahila (2008) and Gritsenko and Aleshinskaya (2016) suggested, to translate songs that are bilingual serves as a means of opening up the lyrics to 'outsiders', etc.

[15] Eclecticism' is a very good way to address multiple topics across academic disciples in an innovative way: https://doi.org/10.17744/mehc.27.1.tf591m8384t50njt

religions

MDPI

Concept Paper

Where Is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth

Suleman Lazarus

School of Humanities and Social Sciences, University of Greenwich, Park Row, London SE10 9LS, UK; suleman.lazarus@gmail.com

Received: 20 January 2019; Accepted: 22 February 2019; Published: 27 February 2019

Abstract: This article is a theoretical treatment of the ways in which local worldviews on wealth acquisition give rise to contemporary manifestations of spirituality in cyberspace. It unpacks spiritual (occult) economies and wealth generation through a historical perspective. The article '*devil advocates*' the 'sainthood' of claimed law-abiding citizens, by highlighting that the line dividing them and the Nigerian cybercriminals (*Yahoo-Boys*) is blurred with regards to the use of magical means for material ends. By doing so, the article also illustrates that the intersectionality of the spirit world and the acquisition of wealth (crime or otherwise) is connected with local epistemologies and worldviews, and its contemporaneity has social security benefits. Therefore, the view that the contemporary manifestations of spirituality in cyberspace signify a 'new-danger' and an ever-increasing outrage in Nigerian society is misplaced. I conclude that if people believe all aspects of life are reflective of the spiritual world and determined by it, the spiritual realm, by implication, is the base of society, upon which sits the superstructure comprised of all aspects of life, especially wealth. Inferentially, this conceptual position that the spirit world is the base of society is an inversion of Orthodox Marxist's theory of economic determinism.

Keywords: sociology of religion; spiritual and magical powers; economic anthropology; gospel of prosperity; Mami Wata or Olokun; digital spiritualization; spiritual manipulation of victims; Nigerian cybercriminals and scams; occult economy; Yahoo Boys and money rituals

1. Introduction

The delinquent may not stand as an alien in the body of society but may represent a disturbing reflection or a caricature instead (Matza and Sykes 1961, p. 717).

Money Doublers and Money Doubling

Spiritual and magical powers, despite the fact that the dominant culture ignores and even denies their reality and contemporaneity, persist and continue to emerge in modern societies (Bever and Styers 2018). While it is of utmost importance to advance our understanding of the spiritual aspects of digital crimes (Melvin and Ayotunde 2010), the spiritual dimension of these crimes is under-theorized. This current endeavor is prompted by the need to urge cyber-fraud researchers to look beyond normal "scientific evidence" and consider the traces of "spiritual manipulations of victims" for material gains that are all too often ignored in "normal social science". A better understanding of this phenomenon lies in our capacity to unconditionally value all insights across the global South and global North (Cross 2018; Lazarus 2018). Indeed, crimes committed on the Internet constitute global issues, with

global consequences (Kirillova et al. 2017), having brought, for example, Nigerian[1] cybercriminals to the attention of the international community (Trend Micro and INTERPOL 2017). This article is broadly based on the premise that Nigerian cybercriminals who use magical/spiritual powers to defraud victims may not be "alien" to the body of society, to use Matza and Sykes's (1961, p. 717) term, but may represent a disturbing reflection or a caricature instead. The word "alien" here means "foreign", i.e., the characteristics of Nigerian society that are not its own. The article, therefore, sets out to trace the roots of contemporary manifestations of spirituality in a Nigerian context.

In order to achieve this, stepping backwards is enlightening. The contemporary manifestation of spirituality in cyberspace has to be analyzed with history in mind, to understand the past that created it. In the 1940s, before the digitalization of social life, many colonial head teachers observed that a group of Nigerian schoolboys (*money doublers*) were diabolic manipulators in trickery and scams (US Consulate 1949). These "money doublers" (*Wayo-Boys*) closely collaborated with indigenous spiritual knowers, such as herbalists or "native doctors" (Igwe 2007). While these "money doublers or Wayo-Boys" were implicated in defrauding many victims in Western societies with scam letters and magical amulets (Nkoh 1963), "money doubling" has always been associated with mystical powers in this context (Ellis 2016). This article, therefore, explores the importance of mystical and spiritual powers in wealth accumulation through the lens of cyber-spiritualism. For Tade (2013), "cyber-spiritualism" is the use of spiritual powers to defraud victims in cyberspace. Analogously, the defrauding of victims for monetary benefits is the most significant theme in the analysis of Nigerian cybercriminals and the "*419-fraud*[2]" thesis (Ibrahim 2016a, 2016b). While many types of cyber-frauds are associated with the broader canon (Button and Cross 2017; Goutam and Verma 2015), the most widely known feature of all of them is 'deception' (Goutam and Verma 2015). The Nigerian cybercriminals, however, are predominantly known for Advance Fee Fraud (Dobovšek et al. 2013) which criminals themselves refer to as a 'game' (Lazarus 2018). Advance Fee Fraud or "419-fraud" is a 'game' for cybercriminals possibly because it embodies not only 'deception' but also includes a range of other characteristics. Such features include the manipulation of victims, the blaming of victims for their predicaments and the "dehumanization of victims" (Lazarus 2018, p. 70). Because Advance Fee Fraud (AFF) encompasses these multiple characteristics, the perpetrator-victim relationship and communication are paramount in the 'game'. Rich's (2018) comprehensive analysis of the Nigerian fraudulent emails, for example, elaborated that victims are commonly deceived into advancing relatively small sums of money in the hope of realising a much larger gain. The online versions of AFF are locally known as '*yahoo-yahoo*[3]' (Akanle et al. 2016). The perpetrators of *yahoo-yahoo* were hence commonly known as "*Yahoo-Boys*" (Ogwezzy 2012). The term *Yahoo-Boys* not only signifies that the perpetrators of the infamous *yahoo-yahoo* are predominantly male (Cross 2018; Lazarus 2018), but also indicates that they are young. Other empirical studies support the youthhood[4] of *Yahoo-Boys* as well (e.g., Aransiola and Asindemade 2011; Lazarus and Okolorie 2019).

In what ways are the actions of youths who tap spiritual resources for online gain a reflection of local epistemologies and worldviews in Nigeria? Are these actions alien in the body of Nigerian society? In attempting to answer these questions, this article will deconstruct the prevailing meaning of cyber-spiritualism in order to stimulate interdisciplinary dialogue. It will do so by weaving together published documents from across a number of disciplinary boundaries (West African poetry,

---

[1] However, critical examinations have pointed out that the statistics the FBI relied upon to inform the currency of cybercrime perpetrators across nations, even when they represent the underlying reality, are socially and selectively constructed, and cannot (or should not) directly speak for themselves (Ibrahim 2016a, pp. 50–52).

[2] The term "419" is historically derived from section 419 of the Nigerian Criminal Code which deals with multiple variations of frauds. Nowadays, "419" is 'loosely' used in everyday parlance as a simple antonym for cheating, falsification and fraudulent representation of facts.

[3] The term '*yahoo-yahoo*' originated from the dominance of Yahoo emails, apps and instant messaging in perpetrator-victim communications.

[4] However, in the public discourse, people above 30 years of age are commonly and culturally seen as "youths"; the meaning of "youths" in Nigeria must be read in terms of the definitions they carry in a Nigerian context.

religious studies, anthropology, sociology, and cultural criminology), to unpack the ways in which local epistemologies and worldviews on wealth acquisition give rise to contemporary manifestations of spirituality in cyberspace. While the inclusion of West African poetry, in particular, may seem strange to some modern sociologists, the sociological eye, as Longo (2015) suggested, can be sharpened by our engagement with literary sources. The deployment of these strategies is prompted by two central motives: (1) to underline that contextual realities on the ground should be taken seriously, beyond their particular geographical and disciplinary contexts; and (2) to underscore that the contextual and cultural realities should inform policymaking in the real world of a spiritually embedded economy.

2. Defining "Digital Spiritualization"

One of these realities is that many Nigerians, like the people before them, believe that the spirit world is the true source of material wealth (Akanle and Adejare 2018; Ellis 2016; Rosen 1989). In particular, many Nigerians believe that no one can succeed in his or her career, whether in crime or legitimate professions, without securing divine blessings, first and foremost, from spiritual beings (Ellis 2016; Rosen 1989). 'There are certain events in life that hard work or physical strength cannot achieve except one understands and possess some spiritual powers[5]' Notably, some qualitative studies have indicated that the Nigerian cybercriminals use magical powers to defraud victims all over the world (Melvin and Ayotunde 2010; Ibrahim 2016b). While some of these studies have implicitly[6] observed the spiritual dimension of cyber-fraud (Aransiola and Asindemade 2011; Ajirola 2015; Ibrahim 2016b; Lazarus and Okolorie 2019), others have explicitly examined the same phenomenon (Melvin and Ayotunde 2010; Tade 2013). In recent years, what is remarkable is that most of these victims are mainly swindled in the context of "love" and "friendship" (Trend Micro and INTERPOL 2017). While some researchers hypothesized that the people who are most susceptible to the romance scam are those who describe themselves as seeking out perfect partners or "true" love (i.e., online profiles) (Whitty et al. 2017), this conjecture did not consider the role of charms and magic in romance-scam victimization. Many cybercriminals (*Yahoo-Boys)* control their "clients" (victims) with various spiritual means, known locally as "*African Jazz*" (Ajirola 2015; Information Nigeria 2017). Such spiritual means include, for example, putting spells on victims' photographs in shrines and communicating with them via the telephone (Information Nigeria 2017) through "*words-of-power*" (Peavy 2016), locally known as "*do-as-I-say*" (Ajirola 2015). The *do-as-I-say* spell or *words-of-power* include the use of verbal postulations to unlock cosmic forces that can make the spiritual manifest itself in the physical realm (Peavy 2016). In this way, spells can be invoked or undone by *words-of-power* or oratory postulations, depending on the invokers' intentions. For example, *words-of-power* could be invoked to enhance or inhibit a person's examination performance (educational-spiritualism), make a person fall in or out of love (love-spiritualism) or help a person recover from illness or become ill (health-spiritualism). Concerning the role of charms and magic in online scam victimization, the narratives of frontline law enforcement officers are revealing. According to Lazarus and Okolorie's (2019, p. 24) study which interviewed 40 Economic and Financial Crimes Commission agents, one of the ritualized practices used by some Nigerian cybercriminals to manipulate their victims is:

> *to put a victim's picture under the laptop* [that is] *after the spiritualist (native doctor) might have "worked on" the picture (cast a spell on it possibly in his/her shrine). It is then necessary and sufficient for fraudsters to simply place the photograph under the computer while chatting/messaging the victims of fraud. Also, in the words of one respondent, "fraudsters also talk to the [victims'] pictures repeatedly" which represent the words-of-power ("do as I say" rhetoric).*

---

5 A direct quote from one of Melvin and Ayotunde (2010, p. 369) participants.

6 Explicit and implicit: for example, Ibrahim (2016b) interviewed 17 parents regarding children's vulnerability to involvement in cybercrime (implicit), whereas Tade (2013) interviewed 10 Yahoo-Boys on the spiritual dimension of cybercrime (explicit). However, while both studies relied on different groups of Nigerians as participants, i.e., parents and Yahoo-Boys, they agreed on the significance of spiritual and magical powers in the discussion of cyber-frauds that emanate from Nigeria.

Yahoo-Boys commonly not only use spiritual means to increase the economic benefit of their fraudulent activities, but also use them as "spiritual insurance" so that no harm may befall them while carrying out their criminal activities (e.g., Adebayo 2013; Lazarus and Okolorie 2019). Based on the preceding remarks, I will henceforth deploy a more critical examination of the existing literature on spirituality in cyberspace, or cyber-spiritualism. While there is a dearth of empirical studies on this topic, my quarrel with the current definition of cyber-spiritualism (Tade 2013) or "spirituality in cyberspace" (Melvin and Ayotunde 2010) is based on three central reasons. In particular, while I build on Tade's (2013, p. 702) and Melvin and Ayotunde's (2010, p. 374) work on spirituality in cyberspace, I disagree with them in three related ways: (1) I question the implicit polarization of the real world and the virtual world, which ignores that cyber-spiritualism has emerged from a well-established origin; (2) I disagree with the assertion that cyber-spiritualism has a singular meaning; and (3) I oppose the negativization of spirituality in the virtual world.

First, Melvin and Ayotunde (2010, p. 364) drew from the Yoruba[7] cultural cosmos (Nigeria) and explained that 'spirituality has been a crucial factor in the activities of offenders involved in both organized and non-organized crimes' in the virtual world. Accordingly, cybercriminals (*Yahoo-Boys*) who defraud their victims using supernatural powers are called "*Yahoo-Boys plus*" (Melvin and Ayotunde 2010). Building on Melvin and Ayotunde's (2010) work, Tade (2013, p. 690) defined cyber-spiritualism as

> *a cybercrime strategy which blends spiritual elements with internet surfing to enhance victimisation rates on the web. Cyber spiritualism involves the procurement and use of mystical, spiritual, and supernatural powers by yahoo boys to cast a spell on their victims. Through this method, victims become hypnotised and, without objection, offer their treasures (products and money) to the fraudsters.*

These lines capture how the author interpreted the meaning of cyber-spiritualism. While the above meaning of cyber-spiritualism does not deal with offline fraud practices, it sheds light on how cybercriminals, through their inventiveness, deployed offline beliefs and practices on the Internet. It is this inventiveness that the above author conceives as alien and, by the same token, the term cyber-spiritualism (this accusation is justified further down). As far as this article is concerned, offline practices predate online ones; the licit and illicit tapping of spiritual resources for wealth acquisition offline predates the use of this practice online, and clarifies the concept of cyber-spiritualism. By the same token, it agrees with the notion that the polarization of the real world and the virtual world obstructs the understanding of socially constructed cues offline, which are concurrently impactful in the digital realm (McGerty 2000; Jaishankar 2007; Powell et al. 2018). Many researchers have indeed highlighted the "life-offline" and "life-online" linkages[8], but they have coined different phrases or joined different sets of words to express the same idea. For example[9], while for McGerty (2000, p. 895) "nobody lives only in cyberspace", for Morahan-Martin (2000, p. 689) "life online is a mere extension of life offline". While Jaishankar (2007, 2011) factored a crime element into the equation and called it "cyber criminology", Powell et al. (2017, 2018) on the one hand renamed Jaishankar's (2011) version as "digital criminology", they on the other hand elaborated on the notion that the "life-offline" and "life-online" are inseparable (e.g., McGerty 2000; Morahan-Martin 2000) and captured this notion as "digital society". While the preceding remarks may not represent the entirety of the above authors' contributions, they help to shed light on the pattern of the body of knowledge on which this current scholarly endeavor leans. Therefore, I argue that this contemporary phenomenon called cyber-spiritualism is, like history, the witness that testifies to the passing of time.[10]

---

[7] 'Yoruba' constitutes one of the main three ethnic groups in Nigeria (the other two are Hausa and Igbo).

[8] The "life-online and life-online" connections are also reminiscent of Goffman's (Goffman [1959] 1990) notion of the "front-stage" and "back-stage" interactions.

[9] This is by no means an exhaustive list of relevant authors on this topic (life-offline and life-online connections) but it gives an indication of the layers of contributions prior to this current endeavor.

[10] Paraphrased from Marcus Cicero's famous words, "history is the witness that testifies to the passing of time".

Second, based on the above remarks, it is conceivable that the historical backdrop to spirituality in cyberspace is indeed the licit or illicit occult economy in society (Comaroff and Comaroff 1999; Jansen 2011). For this article, the occult economy can be understood as the deployment, real or imagined, of magical means for material ends (Comaroff and Comaroff 1999; Jansen 2011; Steinmüller 2011). Accordingly, this inquiry will draw upon indigenous epistemologies and worldviews to challenge the simplistic rendering of cyber-spiritualism in Nigerian society as alien because of the following reasons: (1) cyber-spiritualism has emerged from a well-established origin; (2) spirituality in cyberspace is a reflection of the past that created it. By the same token, cyber-spiritualism has a dual meaning, since it reflects both the "licit" and the "illicit" components of the occult economy from which it has emerged (e.g., spiritually blessing or cursing a person). Cyber-spiritualism, therefore, has, like the occult economy, a dual meaning or two dimensions: licit and illicit. Thus, this current endeavor defines digital spiritualization or cyber-spiritualism as the use of magical and spiritual powers in cyberspace for functional purposes (e.g., online job applications or online examinations) or dysfunctional purposes (e.g., online scamming or online stalking), depending on subscribers' intentions and the circumstances they address. Moreover, cyber-spiritualism concurrently manifests in the physical space. Arguably, Melvin and Ayotunde (2010, p. 374) and Tade (2013, p. 702) err in conceiving cyber-spiritualism as a singularity, and this misconception has implications, such as the negativization of spirituality in cyberspace.

Third, by assuming that cyber-spiritualism has a singular meaning, the above authors fundamentally constructed it as a troubling phenomenon that needs to be addressed or solved (Best 2008, pp. 14–15). The negativization of spirituality in cybercrime is another basis of my quarrel with the prevailing conceptualization of cyber-spiritualism. For example, Tade (2013, p. 702) particularly claimed that "cyber spiritualism portends danger for a developing country like Nigeria. It leads to image battering which impedes development. A way out of this social ill is a genuine restructuring of the social values of Nigerian society". These authors represented cyber-spiritualism as a phenomenon that symbolizes a new societal problem, that "portends danger" (Tade 2013, p. 702) and "calls for concern" (Melvin and Ayotunde 2010, p. 374). The current endeavor does not intend to justify the illicit occult economy in cyberspace. However, it points out that the manifestation of spirituality in cyberspace is a reflection of a broader and widely accepted indigenous spiritual epistemology and worldview in Nigeria (which is contextualized further down). The claim-makers here (Melvin and Ayotunde 2010; Tade 2013) constructed cyber-spiritualism as a phenomenon that should be recognized as troubling or as a social problem (Best 2008; Gabe and Bury 1988). The negativization of spirituality in cybercrime dislocates it from the well-established indigenous worldview from which cyber-spiritualism emerged. Digital spiritualization or cyber-spiritualism is a reflection of the past that created it. By implication, the negativization of cyber-spirituality echoes chronocentrism. Chronocentrism is a "misconception that one's times are paramount, [while] other periods pale in comparison" (Fowles 1977, p. 1). It is referring to the slighting of the past's historical importance, while exaggerating the historical significance (positive or negative) of the present (Rock 2005). Hence, in an attempt to further justify my disagreement with Tade's (2013, pp. 690, 702) and Melvin and Ayotunde's (2010, p. 374) positions, I will explore the occult economy in a variety of different manifestations, namely: (1) The traditional African spiritual system; (2) the *Olokun* deity; (3) the Gospel of Prosperity; and (4) the villagization of the modern public sphere, in order to nuance the intersectionality of the spirit world and the acquisition of wealth.

3. Different Manifestations of the Occult Economy

3.1. Traditional African Spiritual System

The contemporary manifestation, i.e., cyber-spiritualism, serves as an entry point to the intersectionality of the spirit world and the acquisition of wealth in a Nigerian context. Since "a social phenomenon cannot ultimately be understood apart from the cultural context in which it occurs"

(Beirne 1983, p. 373), it is reasonable to consider how it may be a reflection of a broader Traditional African Spiritual System (TASS). The TASS constitutes both the "good" and the "bad" elements, depending on subscribers' intentionality as well as the circumstances they are addressing (Peek 2016; Smalls 2015). In the TASS, all aspects of life, wealth, health, death, and happiness have their roots in the spiritual realm, the authorities therein consisting of a Supreme Being, lesser divinities, ancestors, and spirits (Magezi and Magezi 2017; Peavy 2016). If people have a good relationship with the principal figures in the spirit world, they will be rewarded with wealth, health, happiness, and protection (Smalls 2015; Washington 2012). Conversely, a breakdown of a harmonious relationship between the spirit world and the physical one has adverse consequences for humans (e.g., sickness, barrenness, death) (Peavy 2016; Smalls 2015).

Since all aspects of life are reflective of the spiritual world and determined by it, the spiritual world is, therefore, the base of society, upon which sits the superstructure, comprised of all aspects of life such as material wealth. The conception that the spirit world determines the material conditions is an inversion of Orthodox Marxist's theory of economic determinism. For Marx and Engel's (Marx and Engel 1967) theory of economic determinism, the economy is the base of society that shapes all its institutions such as family, education, government, religion and the media. Simply put, while Marxist's theory positions the economy as the base of society, it situates religion as a part of the superstructure. Conversely, I argue in this article that the spirit world is the base of society, for believers, in a Nigerian context. Nonetheless, for symbolic interactionists, the meanings that things and social objects (persons) have for people form the basis of their actions (Blumer 1969a, 1969a). Equally, a good relationship or a breakdown of a harmonious relationship between the spirit world and the physical one is associated with the broader socio-moral order and indigenous penal thoughts (Assimeng 1986). While indigenous penal thoughts are rooted in the spiritual realm, the centrality of spiritual beings in people's lives is apparent in Assimeng's (1986, p. 49) and Tankebe's (2008, p. 69) notion of "escapelessness" (an aspect of TASS):

> *Escapelessness meant that the ancestral spirits were thought to be all-knowing; no violation of the norms of society escaped their surveillance, and no offender did. The "severity" of sanctions was used to deter the rest of society; the ancestral spirits were thereby upholders of the socio-moral order.*

Hence, some West African literary scholars (Brew 1975; Clark 1975; Okri 1991) reminded us that people are their ancestors; they follow their footsteps and rarely live in "new times". Since spiritual beings were the upholders of law and order, one might be inclined to suggest that the concept of escapelessness might retain its efficacy online, as it does offline in contemporary Nigeria and elsewhere. Equally, given that the meanings that things and social objects (persons) have for people are the basis of their actions (as mentioned earlier), the contemporaneity of escapelessness in the virtual world highlights the value of the interactionist perspective in the area of cybercrime and cybersecurity. Relatedly, it is therefore common for families to go beyond life's physical challenges to assess their spiritual etiology, since every existential problem is rooted in the spiritual realm according to TASS (Peavy 2016; Sogolo 1991; Washington 2012). Essentially, the manifestation of life's problems necessitates inquiries into the spiritual world for remedies. It also provides guidance on relationship maintenance between the two worlds (Peavy 2016; Peek 2016). For example, a person may sacrifice a goat to ancestors for relationship maintenance. It is believed that when the goat is killed, the vital energy that was the goat is released. In turn, the released energy can then be captured and reused in TASS for "good" purposes, such as asking supernatural authorities for healing, prosperity, and other worthy purposes, or for "bad" purposes, such asking them to curse or aggravate people (Smalls 2015).

Cyber-spiritualism, therefore, is "old wine in a new bottle" that connects with the concept of escapelessness in social surveillance. If an individual believes that ancestral spirits are omnipresent and omnipotent, they are omnipresent and omnipotent in their consequences. In fact, legitimacy and conformity to social rules are central to self-regulation (Tyler 1990; Weber [1946] 1992). What is remarkable here is the legitimacy and meaning that spiritual powers hold for a vast, generalizable body of Nigerian society in their unquestioned conformity to rules that are believed to derive from

ancestral spirits and powers. They do not question the legitimacy of the ancestral spirits and gods; they accept their existence, as they perceive themselves as beneficiaries of their rules, all embedded in the concept of escapelessness. For example, most Nigerians would not hesitate to adhere to warning signs associated with "spiritual powers", as shown in Figure 1a,b, because they believe that no offenders can escape their surveillance. The concept of escapelessness could help to facilitate cybersecurity in West Africa, as has been demonstrated in other aspects of security in West Africa from the distant past to the present.

(**a**)

(**b**)

Figure 1. (**a**) Reflections of Escapelessness, (**b**) Reflections of Escapelessness.

Based on the efficacy of spiritual powers as security tools in Nigeria, as shown in Figure 1a,b, I disagree with the mainstream security-principles that repressive technologies (e.g., mass incarcerations) would succeed in Africa, including in Nigeria (see also Cohen 1988; Agozino 2017).

This current article, therefore, advocates for agents of the overall cybersecurity ecosystem to take on board the importance of spirituality in the lives of digital-age Nigerians. While spiritual beings are the true givers of wealth (Ellis 2016), no offender or violation of social norms escapes their surveillance (Tankebe 2008). Because of this, it is conceivable in Nigeria that a central prerequisite for analyzing material welfare is not only an understanding of a person or people's spiritual welfare (Ellis 2016; Kalu 1977), but also an understanding of real-life social security implications (e.g., escapelessness). Having used the TASS to illustrate that cyber-spiritualism has emerged from a well-established indigenous spiritual worldview, I will henceforth draw upon the concept of the *Olokun* deity.

3.2. Olokun

> *So drunken, like ancient walls*
>
> *We crumble in heaps at your feet;*
>
> *And as the good maid of the sea,*
>
> *Full of rich bounties for men,*
>
> *You lift us all beggars to your breast*—Clark (1975, p. 44)

Our engagement with literary sources can sharpen the sociological eye (Longo 2015). As depicted in Clark's (1975) poem above, decoding the name "*Olokun*", popularly known in the global West African diaspora as "*Mami Wata*" (mother of water), is a critical entry point for analyzing spiritual welfare as material welfare in a Nigerian context (Rosen 1989). In the ancient mythology of the Benin kingdom,[11] *Olokun* is considered the giver of material wealth (Peavy 2016). *Olokun* is a critical entry point for understanding the symbolic meaning of the spiritual realm as a real source of economic power in Nigerian communities. *Mami Wata* is the water spirit, culturally and popularly believed to possess immeasurable riches in its kingdom beneath the sea (e.g., in Yoruba, Igbo, and Edo culture in present-day Nigeria) (Rosen 1989; Peavy 2016). Where is the money? If people believe *Mami Wata's* kingdom is where the real[12] money is, *Mami Wata's* kingdom is real in its consequences (Thomas and Thomas 1928). Accordingly, worshippers commonly offer sacrifices to the deity of money for blessings believed to exist in abundance beneath the sea. Therefore, worshippers act based on the meanings *Olokun* has for them. The reciprocal exchanges between families and their "imagined others" in the spirit world are critical to the relationship between them (Falola 1995; Guyer 2004). The mutual exchanges implicitly expressed, such as when praying, or explicitly demonstrated, such as when tithing, ensure the coming and going of souls and things that are all intermingled with one another (Droz and Gez 2015). Notably, the spirit world and the realities of financial success were strongly linked in the social communities that became known as Nigeria[13] (Kalu 1977). For symbolic interactionists, while meanings are the basis of human actions, these are reproduced through interactions with beings (e.g., the water spirit and members of human society) (Blumer 1969a). In a Nigerian context, it is conceivable that these meanings are derived from socio-spiritual interactions.

The significance of *Olokun* in Nigerian culture reinforces the notion that the spirit world is the real source of wealth for adherents who often offer sacrifices. These sacrifices or customary "handshakes" with *Olokun* or *Mami Wata* have reciprocal effects. While the givers may receive earthly wealth, they are indebted to *Olokun* in terms of obedience and further sacrifices (Rosen 1989; Peavy 2016). "Gifts to humans and the gods serve the purpose of buying peace between them both" (Mauss 1925, p. 21). For this article, the meaning of "wealth" is not merely about material wealth (money), but also

---

[11] Contemporary Nigerian society has sprouted from the ruins of three ancient West African kingdoms: the Benin Kingdom, the Bornu Empire, and the Songhai Empire (Ibrahim 2016a).

[12] The encounter of a famous Nigerian singer, Sir Victor Uwaifo, with *Mami Wata* is recounted here: http://www.informationng.com/2015/09/meet-sir-victor-uwaifo-the-nigerian-musician-who-saw-a-real-mermaid-narrates-experience.html.

[13] On 1 January 1914, His Majesty the King of Great Britain amalgamated the Northern and Southern British Protectorates into the colony of Nigeria. Nigeria remained a British colony until 1960 (Lazarus et al. 2017).

encompasses other aspects of life such as fertility, children, good health, and happiness (e.g., Ellis 2016), which helps explain indigenous epistemologies of prosperity. In particular, wealth could come to adherents in the form of fertility and a baby boom in the extended family. Large numbers of children are culturally seen as an essential aspect of wealth. Children are believed to be gifts of the gods, and the significance of children is evident in some Nigerian names[14] (Amadi et al. 2017). By the same token, the contemporaneity of the preceding statements is evident in these Nigerian names[15] (Amadi et al. 2017), which concomitantly explain indigenous epistemologies of prosperity (e.g., in the Yoruba, Igbo, and Edo languages). Nigeria has over five hundred local languages (Lazarus 2018), but these multi-ethnic variations have a historical bond in the spiritual significance of children's names (Amadi et al. 2017).

The spiritual significance of some Nigerian names highlights the notion of wealth that people have. To have large families (wives and children) is an excellent source of wealth. Wealth is strongly associated with mystical and spiritual powers. Consistent with the indigenous epistemologies of prosperity, people who are wealthy were and are presently thought to have special blessings from the invisible world (Falola 1995; Peavy 2016). Large numbers of children manifest by implication in an abundance of material wealth (Peavy 2016). Large numbers of servants and slaves are also symbols of wealth and favor from gods such as *Olokun* (Rosen 1989; Peek 2016). For example, in the pre-colonial era, people who accumulated more wealth than their neighbors were thought to have received special favors from the spirit world (Ellis 2016). Consequently, a farmer who has more land and laborers (e.g., children, wives, slaves, servants) would prosper more than his peers–in terms of land and people (Falola 1995). In fact, as Peavy (2016) explained, some Nigerians believed that no one ever lives without knowing the arch spirit of wealth called *Olokun* or *Mami Wata*, a real symbol of "wealth".

By implication, for believers, no one can buy or sell anything without having to touch and know money, *Olokun*. To have a good relationship with the spirit world guarantees material rewards (children, slaves, and servants); which is an inversion of Orthodox Marxist's theory of economic determinism as previously mentioned. For instance, a slave or a servant represents a store of value, and wealth-in-people could easily translate into wealth-in-money (Ellis 2016; Guyer 2004). Every good relationship requires maintenance. Having strong allies and networks of people were useful assets in the accumulation of wealth, for example when paying (bride prices) for wives or selling/buying slaves for a different purpose, such as valuable items to be sacrificed to the spirit world (Guyer 2004). The preceding comments illuminate how the invisible world becomes central to the acquisition of slaves in pre-colonial Nigeria, and align with the idea that the spirit world is indeed the actual source of wealth. For example, until the late 1950s, the Aro shrine[16] (also known as the long-juju shrine) served as the theocratic administrative machinery (Ellis 2016; Shankland 1933). It also had the power to bless adherents and curse transgressors and their families (Shankland 1933). A fuller analysis of the contemporaneity shrines in modern Nigeria is given below.

A standard method of punishing the convicted—without extending the punishment to the transgressor's family members—was to sell the sentenced into slavery (if the transgressor's "kinsmen" were not able to pay a certain amount of money to the administrative system of the shrine) (Falola 1995). Once such a shrine[17] has turned a person into a slave, it does not matter if the individual was sold or freed by his/her family; that person symbolizes a store of value one way or the other. Some

---

[14] Such as (1) *Oyagbemi* in the Yoruba language, meaning "the goddess has rewarded me"; and *Chukwuyem* in Igbo language, meaning "Almighty God gave me (child)".

[15] Such as (1) *Omosigho* in the Edo language, meaning "a child is more valuable than money"; (2) *Efemena* in the Isoko/Urhobo language, meaning "this one (child) is my wealth"; and (3) *Nwakaego* in the Igbo language, meaning "a child is greater than material wealth".

[16] Whilst the Aro-shrine was geographically located in the Eastern Nigerian region, its spiritual effects extended to present-day Congo and Sierra Leone (Shankland 1933).

[17] Also, similar to '*Trokosi*' spiritual practice in Ghana (another West African country), where any adult who transgresses against the collective sentiment of the village social community submits a young girl from his/her family to the traditional Shrine Priest to labour and serve for 3–5 years in shrines as a way of atonement (Rush and Lazarus 2018).

people believe in the long-juju shrine's power over life and death. By implication, the long-juju shrine is omnipotent in its judgments and consequences. It recalls Thomas and Thomas's (1928) idea that if people believe situations are real, they are real in their consequences. Relatedly, most ritual killings of victims (often slaves) were believed to increase the wealth of the person who offered the sacrifice of the victim to the invisible world, reinforcing the real source of wealth (Agozino 2017; Falola 1995; Kalu 1977). In every conceivable manner, the spirit world is no less significant today than in the Nigerian past. It is reasonable to suggest that the belief that the spirit world is the actual source of wealth is a link to the past and a bridge to our future. For example, the contemporaneity of ritual killings for money success is well documented in various discourses (Aghedo 2015; Agozino 2017; Igbinovia 1988).

In most cases in contemporary Nigeria, as Aghedo (2015, p. 140) explained, the perpetrators would kill the victims and take "vital parts of their bodies" for money rituals. Although the ritual killing of a human is inhuman and gruesome, its contemporaneity in Nigeria also reinforces the indigenous epistemologies about the use of magical powers to "get rich" (Aghedo 2015; Igbinovia 1988). While the use of human body parts for money rituals reflects the "dark side" of magical/spiritual exploitation, it is legally and publicly condemned in Nigerian society. In fact, the killing of a human for money rituals often results in public vigilante justice against the perpetrators, especially in the public discourse (Aghedo 2015). However, the condemnation of ritual killings does not undermine the idea that some Nigerians see spiritual welfare as material welfare (Agozino 2017). Equally, it is noteworthy that not every Nigerian subscribes to the power of the spiritual realm in dictating the outworking of the physical and social domains, be it "good or evil". One may be inclined to presume that most subscribers (e.g., to the *Olokun* deity) would be from Yorubaland or Benin, but this is only due to the prominence of depictions of these groups in the existing literature (Rosen 1989; Peavy 2016). There are no statistical data to support speculations regarding the features of those who tap religious resources for wealth accumulation. Even if such data exist, there is a danger of failing to capture indigenous spiritualities in all their complexity, beyond their physical-geographical context or ethnic groups that are represented or directly implicated in the literature.

A more critical issue is perhaps that subscribers must make a distinction between benevolent and malevolent spiritual agencies, good and evil intentionality. This article does not suggest that the cultural interpretation of the use of spiritualism for licit and illicit ends acts as one and the same. Equally, it does not intend to reify and justify a fraudulent act (*yahoo-yahoo*) that many Nigerians condemn themselves, not least in light of the use of magical/spiritual powers by some *Yahoo-Boys* to defraud victims all over the world. Many Nigerians, for instance, culturally view the use of spiritualism to seek licit favors and blessings such as fertility, promotion, healing, in a positive light. On the flip side, the same cannot be said concerning the use of such spiritualism to attain wealth through ritual killings. For example, according to recent trends in social media, many Nigerians condemned cybercriminals who steal women's panties, sometimes at gun/knife points, for money rituals[18] The financial realities of women's panties in Nigeria are reflective of a spiritually embedded economy and also reinforce that indeed, the spirit world is the real source of wealth. Nonetheless, the preceding remarks on the concept of the *Olokun* deity shed light on how cyber-spiritualism may have emerged—it could be seen as a reflection of the past that created it. Utilizing a historical perspective, I have used the concept of the *Olokun* deity to argue that the allure and reproduction of mystical/spiritual agency and its appropriation by cybercriminals (*Yahoo-boys*) in their virtual transactions reflect a well-established socio-spiritual script in the discourse on wealth accumulation in Nigeria. By implication, digital spiritualization is the intersectionality of the spirit world and the acquisition of wealth in cyberspace. I will henceforward draw on the concept of the "Gospel of Prosperity" (Adogame 2010; Heuser 2016; Kangwa 2016; Lausanne Theology Working Group 2010) to further contextualize this intersectionality.

---

[18] Media sources such as, "Fear of 'Yahoo boys', ritualists forced female students in Delta state tertiary schools to stop wearing pants": https://www.legit.ng/1211206-fear-yahoo-boys-ritualists-forced-female-students-delta-state-tertiary-schools-stop-wearing-pants.html.

3.3. The Gospel of Prosperity

Historically, the Nigerian religious landscape, representing West Africa, has metamorphosed from the debris of beliefs/practices in the pre-colonial era into a multiplicity of religious traditions (Adogame 2010; Adogame et al. 2012; Heuser 2016; Magezi and Magezi 2017). This multitude of religiosities includes the indigenous religions (embodying shrines) and the Abrahamic religions, i.e., various strands of Christianity and Islam (Kangwa 2016). I draw mainly upon African Christianity, due to the significance of the "Gospel of Prosperity" (Heuser 2016; Lausanne Theology Working Group 2010) in teasing out much of the innovative energy in prosperity-oriented faith in God. The Gospel of Prosperity involves the power of divination, offerings, tithing, and material-prosperity oriented "prayers" (Csordas 2009; Kangwa 2016). Symbolically, these interactions with the imagined others (e.g., offering, tithing, praying) merge the spirit world and the physical world (Heuser 2016). As Nigerian sociocultural relationships are codified and guaranteed via the spirit world (Washington 2012), loyalty and "tithing" are essential aspects of social relationships and Nigerian sociocultural identity, and serve to bind modern-day Nigerians and their "kinsmen" (Ellis 2016). In gift giving (e.g., offering and tithing), the honor of giver and recipient is reciprocally engaged (Mauss 1925). For Droz and Gez (2015), gift exchanges, offering, and tithing are a form of ritualized bonding between believers and God. The critical point here is that quest for wealth-oriented mystical manipulation, which is a reflection of TASS, is a specific aspect of multiple strands of African Christianity in contemporary Nigerian society (Amanze 2013; Magezi and Magezi 2017). One may say that culture is an interwoven set of beliefs and practices that define people's way of life. Unlike DNA, culture is not innate or embedded in the chromosomes, but like DNA, it is a reflection of ancestral faces[19]. African Christianity is not immune to local epistemologies of wealth acquisition (Amanze 2013). For Kangwa (2016), African churches, including Nigerian churches, embody a culture of continuity by reproducing an identifiable character and regaining a pneumatic and charismatic religiosity that existed in traditional African society with their prophetic energy.

The power of divination connection with occult economies is central to traditional African society (Jansen 2011; Kangwa 2016). The power of clairvoyance is the conveyor belt on which the present life situation is transported to the future, so that glimpses of the future can direct the current waves of present life events (Jansen 2011; Peek 1991). At the core of divinity lies the power of the word (Washington 2012), and the practices of the oracular words (*words-of-power*) are commonplace in Nigeria (Ellis 2016). To fully understand the concept of *words-of-power*, we must examine the intentionality that created it (benevolent or malevolent). Depending on the issues the concept of *words-of-power* is invoked to address, the use of *words-of-power* in itself is not an inherently immoral act. While the featuring or absence of prophecy and *words-of-power* in churches determines their growth, pastors who can prophesize and work miracles with oracular *words-of-power* undoubtedly would have more followers than their peers (Kangwa 2016). Indeed, *words-of-power* is a critical tool in the success or failure of the Gospel of Prosperity, which lies at the core of African Christianity. Where is the money? The spirit world is a true source of wealth in modern Nigerian churches (Akanle and Adejare 2018, p. 7) (and as emphasized elsewhere, by implication, cyber-spiritualism may not be an alien in the body of Nigerian society). Similarly, Kangwa (2016, p. 4) observed:

> *Material blessings (fertility and children, good health, secure shelter, plentiful harvests) are explained as signs of divine blessing. Conversely, the root of all problems is spiritual and, therefore, the solution must also be spiritual. If one cannot overcome by oneself the forces that hinder success, one has to look for assistance from those who have the power needed to summon or manipulate spiritual forces.*

For example, there is an elaborate procedure for selecting a spouse, and it is not uncommon for families of spouses-to-be to ascertain that their family-in-law-to-be does not suffer from curses or

[19] Paraphrased from James Small's sentence, during one of his public speeches on "Occult".

illnesses such as leprosy, and/or is not noted for witchery/wizardry. In particular, such investigation of the affine is often done by exploiting the spirit world, to expose the future and the hidden history of their family-in-law-to-be (Amponsah et al. 2006). Also, Chinwoke Mbadinuju, the governor of Anambra state in Nigeria (1999–2003), ordered members of his cabinet to swear an oath of loyalty at an Okija-shrine[20] to ensure the influx of his "assorted" gifts, and they did (Ellis 2016; Ujumadu 2015). There is no statistical data to estimate the numbers of law-abiding citizens who tap religious resources for wealth accumulation. However, it is not uncommon for claimed Christians who are in politics in Nigeria, from local councilors to presidential candidates, to exploit the spirit world via pastors and native doctors as a critical part of election preparation and career enhancement (Ellis 2016). There is no objective viewpoint to critique or compliment this as an "immoral" act (Becker [1974] 1967; Reiner 2016).

Besides, cyber-spiritualism has a dual meaning. Its "good" and "bad" components depend on subscribers' intentionality as well as the circumstances and life problems they are invoked to address. Like claimed law-abiding Nigerians, *Yahoo-Boys*, far from deviating, conform to the commonly held indigenous worldview. So, in "*devil advocating*"[21] the "sainthood" of claimed law-abiding citizens, the argument's critical point here is that the motivations informing spirituality in cyberspace (or in any form of the licit/illicit occult economy, for that matter) are based on local epistemologies and worldviews. For example, Lazarus's (2018) study on the representations[22] of *Yahoo-Boys* in hip-hop music is revealing, because it demonstrated that the *Yahoo-Boys*' embodiment of spirituality is reminiscent of the Gospel of Prosperity. In this study (Lazarus 2018, p. 73):

> *a singer, Kelly Handsome, depicted Yahoo-Boys as follows, " . . . Maga don pay/ Mugu don pay/shout hallelujah . . . / . . . hallelujah hallelujah owo . . . / . . . / . . . hallelujah hallelujah ego . . . / . . . hallelujah, hallelujah kudi, kudi . . . /I don suffer, but I now don hammer, papa God don bless me, no one can change it . . . / . . . ". (The gullible has paid, the senseless has remitted/shout hallelujah . . . / . . . hallelujah, hallelujah money . . . / . . . hallelujah, hallelujah money . . . / . . . /hallelujah, hallelujah money, money . . . I have suffered a lot, but now I have hit the jackpot, Almighty God has blessed me, [and] no one can change it).*

Considering the biblical allusion above (i.e., a reference to the Bible regarding prosperity as a critical element of religiosity), the line dividing cybercriminals and claimed law-abiding Nigerians is blurred. In other words, with regards to the use of spiritual and magical powers for wealth acquisition, the seeming distinction between cybercriminals and claimed law-abiding Nigerians is far from straightforward. The preceding remarks further suggest that cyber-spiritualism cannot ultimately be understood apart from the sociocultural context in which it occurs (because it has a history). Equally, the bottom line here is that material gain is a prime motivation for cyber-spiritualism on the one hand. On the other hand, the notion that the spirit world is the true source of wealth is an inversion of Orthodox Marxist's theory of economic determinism as previously mentioned. Having used the Gospel of Prosperity to contextualize cyber-spiritualism, I henceforth use the analysis of Kalu (2002) and his term "the villagization of the modern public sphere" to nuance the intersectionality of the spirit world and the acquisition of wealth.

---

[20] Over 70 human bodies and skulls were discovered on the premises of the Okija-shrine in 2015 (covering about a decade).

[21] Here, the phrase "devil advocating", means arguing against the 'righteousness' or 'sainthood' of a group (claimed law-abiding citizens) in order to uncover any misrepresentation of the evidence favouring them (e.g., concerning the use of magical/spiritual powers for wealth generation).

[22] It is noteworthy that the representation of fraudsters by Nigerian singers predates the digitalization of fraud. For example, a singer, Ogbogu Okonji, in his song "Alusi Ego", meaning the god(dess) of money, personified Fred Ajedua (an alleged 419-fraud kingpin in the 1990s) as follows (translated from Enuani to English): " . . . /Fred-o! who is like Fred-o!/the God of money, who is like Fred-o/ . . . /The sun that shines for the masses/who is like Fred-o!/ . . . / . . . ".

3.4. The Villagization of the Modern Public Sphere

Contemporary Nigerian identities could be seen as Janus-faced. For example, irrespective of the primacy of Christianity or other religions in people's lives, most ethnic groups in Nigeria bury their dead according to indigenous spiritual worldviews and rituals (Ellis 2016). While such burial rites are major community events (Ibrahim 2015; Peavy 2016), they are primarily intended to nurture the relationship between the ancestral spirits and the human family (relationship maintenance is one of the most crucial aspects of material welfare) (Peavy 2016). Drawing from Ekeh (1975), Kalu (2002, p. 674) coined the term "the villagization of the modern public sphere" to describe the Janus-faced identity of modern Nigerians. For Kalu (2002, p. 674), most modern Nigerians are "as viruses feeding on the red blood corpuscles of the primal world and spiritual shrines in rural areas". According to Ekeh's (1975) original formulations, modern Nigerians simultaneously live in two opposed yet intersecting public spheres. The first involves influences from cultural beliefs and practices (e.g., burial rites). It is a local sphere made up of strong bonds of kinship located in villages and the birthplaces and shrines therein. The second sphere is that constituted by colonial endeavors such as the national assembly, parliament, federal government, and the national press. The historical, political, and sociocultural context of Nigeria merged these two spheres, which revolve around familial ties and places of origin or nativity.

Within the Nigerian cultural realm, kinship-nurturing is commonplace (Ibrahim 2015). A man may be the most powerful person in the nation politically, but he is socioculturally indebted to his place of origin. The client-patron relationship between people in the villages/towns (gatekeepers of the shrines and sacred sites) and the holders of political power and national resources is reciprocal (Ekeh 1975). This reciprocity can be understood through an African proverb: "the left-hand washes the right-hand, and the right one washes the left one and both become clean". By implication, "people's socioeconomic insecurity necessitates a strong rather than less reliance on ties to family and community" (Ibrahim 2015, p. 316). People's strong reliance on families and communities also helped vitalize "the villagization of the modern public sphere" exemplified in public-fund embezzlements and spiritual shrine consultations (Ekeh 1975). In this way, national resources are funneled down to one's place of origin, for personal purposes—with impunity[23].

The cultural and symbolic "hand washing" not only helps harness unity, but also blurs the boundary between the meaning of "bribe" and that of "*dash*" (Ellis 2016; Osoba 1996). While the sociocultural delineation between the two words is not a sharp line, a "*dash*" is a local term for a gift in a Nigerian context. Contexts are a resource for understanding any social phenomenon (Goffman [1959] 1990; Morris 2018). Since in a Nigerian context a "bribe", from a cultural, social, or political lens, can be a "*dash*", it would not be a far stretch to maintain that a "bribe" is a "*dash*" and a "*dash*" is a "bribe", depending on the givers' intentions as well as the circumstances or life problems they are given to address. While metaphor establishes the basis of people's everyday comprehension of life (Santa Ana 2002), I argue that it diffuses the meaning of *dash* and bribe in a Nigerian context. This is because of the following reasons: Although "corruption is a symptom and outcome of institutional deficiency" (Dasgupta and Ugur 2011, p. 2), expertise in bribery has hitherto been deemed necessary and sufficient for political candidates and public post applicants in order for them to be successful in Nigeria (Ellis 2016). Given that in a Nigerian context earthly riches are commonly believed to have spiritual etiology, this worldview on earthly riches has consequences. Some spiritualists and "native doctors" are caught up in the web of bribery (Ibrahim 2016b) within the networks of what Andreski (Stanislav [1968] 1996) called kleptocracy (Stanislav [1968] 1996). Kleptocracy can be defined as a system where the "functioning of the organs of authority is determined by the mechanism of supply and demand rather than the law and regulations", and kleptocrats are the principal social actors in

[23] The 'impunity' here implies that under some institutional umbrellas, as Lazarus's (2019, p. 1) literary work depicted, "the fraudsters are also in charge of fraud-taskforce".

kleptocracies (Stanislav [1968] 1996, p. 109; Osoba 1996, p. 378). For example, the expenditure of large amounts of money and spiritual engagements to acquire a political post has by the same token transformed such political positions into market commodities (Joseph 1987; Osoba 1996). In turn, "market commodities" will inevitably be exploited in to repay any "debts" incurred, in addition to furthering profits and mystical exploitations needed to finance subsequent elections or senior civil-service posts. The foregoing remarks shed light on how cyber-spiritualism may have emerged. By the same token, it also suggests that political corruption is commonplace in Nigeria.

Kalu (2002) and Ekeh (1975) explained that shrines are invaluable political mechanisms for mobilizing economic and sociocultural power in the modern sector and contemporary government offices. For example, it is not uncommon for civil servants or politicians to use the public funds in their possession to finance "worthy" causes in their birthplaces and regularly contribute to the treasury of their "kinsmen" (Ellis 2016). The holders of public posts require spiritual, political, and social support from their places of origin, and their "kinsmen" in the villages can then tap into the economic resources available to politicians and/or holders of public posts (Ekeh 1975; Kalu 2002). Equally, as part of their sacerdotal duties, the gatekeepers of shrines render spiritual services to people (their symbolic sons and daughters) in government and civil service. Reciprocally, the spiritualists gain access to the immense wealth available to the holders of public offices such as those of politicians. Arguably, in Nigeria, as Ellis (2016, p. 195) noted, traditional shrines and churches can be conceptualized as "lubricants of political, civil, and commercial relationships". In this way, meanings of the spirit world as the true source of wealth are continuously produced and reproduced through interactional processes between holders of public posts and chief priests in villages/towns (Blumer 1969a; Carter and Fuller 2016). The above discussion illuminates how and to what extent the relationship between the spiritualists and the holders of public offices in Nigeria forms a critical dynamic in the construction and negotiation of identity and belonging. It also illuminates Kalu's (2002) idea that modern Nigerians could be viewed as "feeding on the red blood corpuscles of the primal world and spiritual shrines in rural areas", as mentioned.

The symbolic meaning of this idea not only reinforces the notion that the spirit world is the true source of material wealth, but also underscores that material wealth embodies not only a mechanical reflection but the imputed sentiments as well. For (Cooley 1992, [1909] 1998), the thing that moves us to our pride or 'shame is not the mere mechanical reflection of ourselves, but an imputed sentiment, and the imagined effect of this reflection upon another's mind—our people'. Arguably, most Nigerians perceive the spirit world (shrines) in their places of origin and their "kinsmen" (keepers of the shrines) as a vital source of legitimacy, a meaningful life, and symbolic sources of their wealth. Similarly, shrine keepers and "kinsmen" see their sons/daughters in public offices as symbols of pride, prestige, and ultimately, sources of wealth (Ekeh 1975). "*Ancestral faces saw us, And said: They have not changed*!" (Brew 1975, p. 43). Some core aspects of culture are transmitted from generation to generation (Ibrahim 2015; Smalls 2015), and as Brew's (1975) poem depicted above, people are reflections of their ancestral faces. With the aim of tapping spiritual recourses for wealth acquisition, most individuals, families, and villages, regardless of their proclamations of Christianity or other dominant religiosities, have shrines within their residential areas and beyond—gateways to communicate with their ancestors, such as during burial or festive ceremonies. I challenge the simplistic rendering of cyber-spiritualism and indigenous epistemologies in Nigeria as distinctly separate entities with easily defined boundaries, because the polarization of the real world and the virtual world obstructs the understanding of licit cyber-behavior and cybercrime.

4. Summary

First, to recapitulate, the use of spiritual powers for financial success is in itself not exclusive to *yahoo-yahoo* enterprises, but represents a reflection of the broader Nigerian society that created it. By implication, cyber-spiritualism may not be an alien in the body of Nigerian society. Indeed, concerning the licit and illicit tapping of spiritual resources for wealth acquisition, "the line dividing good and evil

cuts through the heart of every human being",[24] and this line is thin. Spirituality in the virtual world is an extension of cultural nuances in society, and the tapping of spiritual resources for wealth acquisition is no less critical to cyber criminality than it is to claimed law-abiding citizenship. Yet, claim-makers Tade (2013) and Melvin and Ayotunde (2010) demonized *Yahoo-Boys*, as in Best's (2008, p. 14) words "a social problem", simply for their involvement in the occult economy in the virtual world. I argue that the relationship between its users, whether cybercriminals or law-abiding citizens, is far more complicated than hitherto portrayed in prevailing scholarship. I also argue that the significance of the spirit world and its connections to the acquisition of wealth online are reflections of well-established indigenous spiritual worldviews in Nigerian society.

The significance of the dual meaning of cyber-spiritualism necessitates a more critical examination of cultural boundaries between law-abiding Nigerians and *Yahoo-Boys*. If we conceive cyber-spiritualism as a singularity (as having only one dimension), the problem is that we would be led to conclude that cyber-mysticism is an inherently negative phenomenon. This current endeavour argues that cyber-spiritualism embodies dual meanings (the good and the bad) depending on subscribers' intentionality as well as the circumstances and life problems they address. It reinforces the notion that the centrality of the spirit world as a real source of wealth is no less significant to the ethos of law-abiding citizens of Nigerian society than to that of the *Yahoo-Boys*. This notion, in particular, suggests problems with the prevailing definition of cyber-spiritualism. The "good" and the "bad" components of cyber-spiritualism have previously been taken for granted as only a negative phenomenon, whereas the dual meaning of cyber-spiritualism has implications. Cyber-spiritualism may not in itself "batter the image of Nigeria", as Tade (2013, p. 702) argued. The identification of cyber-spiritualism in cybercrime scholarship simply reinforces the view that spiritual welfare is analogous to material welfare in Nigerian society (Ekeh 1975; Kalu 2002). It is reasonable then to concede that "economic benefits and wealth generation are the primary motives for cybercrime in a Nigerian context" (Ibrahim 2016a, p. 51). Indeed, Yahoo-Boys' deployment of magical and spiritual powers to cast spells on victims in the virtual world is reflective of the connections between the spirit world and the acquisition of wealth in Nigerian society.

5. Conclusions

To understand cyber-spiritualism, I have examined the past that created it and found that contemporary manifestations of spirituality in cyberspace (life-online) are a reflection of local epistemologies and worldviews in society (life-offline). In particular, I explored the occult economy in a variety of different manifestations (TASS, *Olokun* deity, the Gospel of Prosperity, and the villagization of the modern public sphere) in order to demonstrate the intersectionality of the spirit world and the acquisition of wealth, which goes back a long way in Nigerian society. I have proposed that the spiritual world is the base of Nigerian society, upon which the superstructure comprised of all aspects of life, especially wealth, sits. Theoretically, this viewpoint that the spirit world is the base of society, indeed, is an inversion of Orthodox Marxist's theory of economic determinism.

Additionally, I have pointed out that the existing definition of cyber-spiritualism is a recipe for confusion, as it acknowledges only one dimension, and then negativizes it. I have redefined cyber-spiritualism and proposed that it has dual meanings (the good and the bad), like the concept of TASS. Consequently, I have challenged the simplistic rendering of cyber-spiritualism and indigenous epistemologies in Nigeria as distinctly separate entities with easily defined boundaries. In *devil advocating* the righteousness of claimed law-abiding citizens, I highlighted that the seeming distinctions between them and cybercriminals are blurred with regards to the use of mystical powers to increase material wealth. Where is the money? 'Wealth' is rooted in the spirit world. The centrality of the spirit world in wealth acquisition in the physical realm in Nigeria is reflected in the *Yahoo-Boys*' modus

[24] A famous quote from the Russian scholar Aleksandr Solzhenitsyn.

operandi in cyberspace. Thus, I have demonstrated that the discrepancies between its users (whether *Yahoo-Boys* or claimed law-abiding citizens) are far from straightforward. In this context, economic actions are always and inevitably sociocultural actions. They should be interpreted and judged as such. By exploring the moral foundations of economic action (licit/illicit), I have argued that it is misplaced to see *Yahoo-Boys*' exploitations of spiritual powers in cyberspace as signifying "new danger" and an ever-increasing outrage in Nigerian society. *Yahoo-Boys'* exploitation of spiritual/magical powers in the virtual world not only aligns with local epistemologies and worldviews on wealth and prosperity, but also highlights that cybercrime in a Nigerian context is rooted in socioeconomics, whose success (like that of licit professions) requires spiritual blessings.

Finally, examining the spiritually embedded economy in all of its complexities would be undermined if tethered to one or two disciplinary contexts and traditions. In this article, I therefore attempted to stimulate an interdisciplinary dialogue between sociology, religious studies, anthropology, and cultural criminology. Analyzing digital spiritualization and contextualizing it within frameworks of traditional and Pentecostal concepts of prosperity and kinship—which may (or may not) develop into practices of political corruption and criminality—is a highly appropriate topic that is underrepresented in research on the intersectionality of religion and economic actions in Africa (or anywhere, for that matter). Contextual and cultural realities on the ground should inform policymaking for information technologies in West Africa, including Nigeria.

The intersectionality of the spirit world and the acquisition of wealth (illicit or licit) are connected with local epistemologies and worldviews, and their contemporaneity has social security benefits through the concept of escapelessness. On a policy level, if digital-age West Africans believe that the spirit world is the true source of wealth and that no offender escapes the punishment of their ancestral spirits and gods (escapelessness), these beliefs have direct policy implications for socioeconomic, cybersecurity, and religious issues in West Africa and elsewhere. In dealing with the historical and foundational issues of socioeconomics and wealth generation, I underscored that life-online is a mere extension of life-offline. A policy conclusion from this article, therefore, is that the above insights from this research could deepen our understanding of the ways local epistemologies and worldviews on wealth acquisition give rise to contemporary manifestations of spirituality in the virtual world. Also, insights from this research could deepen our understanding of the spiritual dynamics of the relationship between *Yahoo-Boys* and their victims all over the world. A better understanding of this type of online fraud can be achieved when we unconditionally value, sponsor, and share all insights from across the global South and the global North, as Lazarus (2018) and Cross (2018) have suggested. I, therefore, urge cyber-fraud researchers to look beyond normal "scientific evidence" and consider the traces of "spiritual manipulations of victims" for material gains that are all too often ignored in "normal social science".

Funding: This research received no external funding.

Acknowledgments: I thank Afe Adogame, Tim Hall, and the anonymous referees for their insightful suggestions. I also thank Stephen Wyatt and Jeffrey Marck for their gratis efforts in proofreading portions of this article.

Conflicts of Interest: The author declares no conflict of interest.

References

Adebayo, Anthony Abayomi. 2013. Youths' unemployment and crime in Nigeria: A nexus and implications for national development. *International Journal of Sociology and Anthropology* 5: 350. [CrossRef]

Adogame, Afe. 2010. How God became a Nigerian: Religious impulse and the unfolding of a nation. *Journal of Contemporary African Studies* 28: 479–98. [CrossRef]

Adogame, Afeosemime, Ezra Chitando, and Bolaji Bateye. 2012. *African Traditions in the Study of Religion in Africa: Emerging Trends, Indigenous Spirituality and the Interface with Other World Religions*. London: Ashgate Publishing, Ltd.

Aghedo, Iro. 2015. Sowing peace, reaping violence: Understanding the resurgence of kidnapping in post-amnesty Niger Delta, Nigeria. *Insight on Africa* 7: 137–53. [CrossRef]

Agozino, Biko. 2017. Critical Perspectives on Deviance and Social Control in Rural Africa. *African Journal of Criminology and Justice Studies: AJCJS* 10: I.

Ajirola, Felix Oludare. 2015. Globalisation and the Nigerian Youths. Available online: https://www.researchgate.net/publication/281069059_GLOBALIZATION_AFRICAN_CULTURE_AND_JUVENILE_DELINQUENCY (accessed on 26 September 2018).

Akanle, Olayinka, and Gbenga S. Adejare. 2018. Contextualizing Pentecostal Gatherings in Southwestern Nigeria: Social Drivers and Significance. In *Religion in Context*. Baden-Baden: Nomos Verlagsgesellschaft, pp. 145–58.

Akanle, Olayinka, J. O. Adesina, and E. P. Akarah. 2016. Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria. *African Journal of Science, Technology, Innovation and Development* 8: 213–20. [CrossRef]

Amadi, Richard Nlemanya, Efetobor O. Elijah, and Grace Nnennaya Nwaubeta. 2017. Rethinking the etiology of names as communication channels in Nigeria. *International Journal of Research and Development Studies* 8: 1–15.

Amanze, James N. 2013. The role of prophecy in the growth and expansion of the Synagogue Church of All Na ons. *Scriptura* 112: 1–14. [CrossRef]

Amponsah, Benjamin, Charity Akotia, and Akinsola Olowu. 2006. Ghana. In *Families across Cultures: A 30-Nation Psychological Study*. Edited by James Georgas, John W. Berry, Fons J. van de Vijver, Çigdem Kagitçibasi and Ype H. Poortinga. Cambridge: Cambridge University Press.

Aransiola, Joshua Oyeniyi, and Suraj Olalekan Asindemade. 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking* 14: 759–63. [CrossRef] [PubMed]

Assimeng, Max. 1986. *Social Structure of Ghana*. Accra: Ghana Universities Press.

Becker, Howard S. 1997. *Outsiders: Studies in Sociology of Deviance*. New York: Simon and Schuster Ltd. First published 1967.

Beirne, Piers. 1983. Cultural relativism and comparative criminology. *Crime, Law and Social Change* 7: 371–91. [CrossRef]

Best, Joel. 2008. *Social Problems*. New York: WW Norton.

Bever, Edward, and Randall Styers. 2018. *Magic in the Modern World*. Pennsylvania: Pennsylvania State University Press.

Blumer, Herbert. 1969a. *Symbolic Interactionism: Perspective and Method*. Eaglewood Cliffs: Prentice Hall.

Blumer, Herbert. 1969b. *The Methodological Position of Symbolic Interactionism', in Symbolic Interaction*. Eaglewood Cliffs: Prentice-Hall.

Brew, Kwesi. 1975. Ancestral Faces. In *Poems of Black Africa*. Edited by Wole Soyinka. London: Heinemann Educational Books Ltd., p. 43.

Button, Mark, and Cassandra Cross. 2017. *Cyber Frauds, Scams and Their Victims*. New York: Taylor & Francis.

Carter, Michael J., and Celene Fuller. 2016. Symbols, meaning, and action: The past, present, and future of symbolic interactionism. *Current Sociology* 64: 931–61. [CrossRef]

Clark, John Pepper. 1975. Olokun. In *Poems of Black Africa*. Edited by Wole Soyinka. London: Heinemann Educational Books Ltd., pp. 43–44.

Cohen, Stanley. 1988. *Against Criminology*. New Brunswick: Transaction.

Comaroff, Jean, and John L. Comaroff. 1999. Occult economies and the violence of abstraction: Notes from the South African postcolony. *American Ethnologist* 26: 279–303. [CrossRef]

Cooley, Charles Horton. 1998. *On Self and Social Organisation*. Chicago: The University of Chicago Press. First published 1909.

Cooley, Charles Horton. 1992. *Human Nature and the Social Order*. London: Transaction Publishers.

Cross, Cassandra. 2018. Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In *The Palgrave Handbook of Criminology and the Global South*. Cham: Palgrave Macmillan, pp. 261–80.

Csordas, Thomas J., ed. 2009. Introduction: Modalies of transnational transcendence. In *Transnational Transcendence: Essays on Religion and Globalisation*. Berkeley: University of California Press, pp. 1–29.

Dasgupta, Nandini, and Mehmet Ugur. 2011. *Evidence on the Economic Growth Impacts of Corruption in Low-Income Countries and Beyond: A Systematic Review*. London: EPPI-Centre, Social Science Research Unit, Institute of Education, University of London.

Dobovšek, Bojan, Igor Lamberger, and Boštjan Slak. 2013. Advance fee frauds messages–non-declining trend. *Journal of Money Laundering Control* 16: 209–30. [CrossRef]

Droz, Yvan, and Yonatan Gez. 2015. A god trap: Seed planting, gift logic, and the prosperity gospel. In *Pastures of Plenty: Tracing Religio-Scapes of Prosperity Gospel in Africa and Beyond*. Edited by Andreas Heuser. Frankfurt: Lang, pp. 295–307.

Ekeh, Peter P. 1975. Colonialism and the two publics in Africa: A theoretical statement. *Comparative Studies in Society and History* 17: 91–112. [CrossRef]

Ellis, Stephen. 2016. *This Present Darkness: A History of Nigerian Organized Crime*. Oxford: Oxford University Press.

Falola, Toyin. 1995. Money and Informal Credit Institutions in Colonial Western Nigeria. In *Money Matters: Instability, Values and Social Payment in the Modern History of West African Communities*. Edited by Jane Guyer. London: James Currey, pp. 162–87.

Fowles, Jib. 1977. The problem of values in futures research. *Futures* 9: 303–14. [CrossRef]

Gabe, Jonathan, and Michael Bury. 1988. Tranquillisers as a social problem. *The Sociological Review* 36: 320–52. [CrossRef]

Goffman, Erving. 1990. *The Presentation of Self in Everyday Life*. New York: Doubleday. First published 1959.

Goutam, Rajesh Kumar, and Deepak Kumar Verma. 2015. Top Five Cyber Frauds. *International Journal of Computer Applications* 119: 23–25. [CrossRef]

Guyer, Jane. 2004. *Marginal Gains: Monetary Transactions in Atlantic Africa*. Chicago: Chicago University Press.

Heuser, Andreas. 2016. Charting African Prosperity Gospel economies. *HTS Theological Studies* 72: 1–9. [CrossRef]

Ibrahim, Suleman. 2015. A Binary Model of Broken Home: Parental Death-Divorce Hypothesis of Male Juvenile Delinquency in Nigeria and Ghana. In *Contemporary Perspectives in Family Research*. Edited by Sheila Royo Maxwell and Sampson Lee Blair. New York: Emerald Group Publishing Limited, vol. 9, pp. 311–40.

Ibrahim, Suleman. 2016a. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice* 47: 44–57. [CrossRef]

Ibrahim, Suleman. 2016b. Causes of socioeconomic cybercrime in Nigeria. Paper presented at IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada, June 12–14; pp. 1–9.

Igbinovia, Patrick Edobor. 1988. Ritual murders in Nigeria. *International Journal of Offender Therapy and Comparative Criminology* 32: 37–43. [CrossRef]

Igwe, Chidi Nnamdi. 2007. *Taking Back Nigeria from 419: What to Do about the Worldwide E-mail Scam—Advance-Fee Fraud*. Toronto: iUniverse.

Information Nigeria. 2017. Girls Run Mad. Available online: http://www.informationng.com/2017/07/girls-run-mad-become-useless-use-yahoo-plus-yahoo-boys-confesses.html (accessed on 20 January 2018).

Jaishankar, Karuppannan. 2007. Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology* 1: 1–6.

Jaishankar, Karuppannan, ed. 2011. Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton: CRC Press, pp. xxvii–xxxv.

Jansen, Jan. 2011. Framing divination: A Mande divination expert and the occult economy. *Africa* 79: 110–27. [CrossRef]

Joseph, Richard A. 1987. *Democracy and Prebendal Politics in Nigeria: The Rise and Fall of the Second Republic*. Cambridge: Cambridge University Press.

Kalu, O. U. 1977. Missionaries, Colonial Government and Secret Societies in South-Eastern Igboland, 1920–1950. *Journal of the Historical Society of Nigeria* 9: 75–90.

Kalu, Ogbu U. 2002. The Religious Dimension of the Legitimacy Crisis, 1993–1998. In *Nigeria in the Twentieth Century*. Edited by Toyin Falola. Durham: Carolina Academics Press, pp. 667–85.

Kangwa, Jonathan. 2016. The role of the theology of retribution in the growth of Pentecostal-Charismatic churches in Africa. *Verbum et Ecclesia* 37: 1–9. [CrossRef]

Kirillova, Elena Anatolyevna, Rashad Afatovich Kurbanov, Natalia Viktorovna Svechnikova, Teymur El'darovich Zul'fugarzade, and Sergey Sergeevich Zenin. 2017. Problems of Fighting Crimes on the Internet. *Journal of Advanced Research in Law and Economics* 8: 849–56.

Lausanne Theology Working Group. 2010. A Statement on the Prosperity Gospel. Available online: https://www.lausanne.org/content/a-statement-on-the-prosperity-gospel (accessed on 7 July 2018).

Lazarus, Suleman. 2018. Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists. *Criminology, Criminal Justice, Law & Society* 19: 63–80.

Lazarus, Suleman. 2019. Betrayals in Academia and a Black Demon from Ephesus. *Wisdom in Education* 9: 1–2.
Lazarus, Suleman, and Geoffrey Uzoma Okolorie. 2019. The Bifurcation of Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. Available online: https://ssrn.com/abstract=3331970 (accessed on 8 February 2019).
Lazarus, Suleman Ibrahim, Michael Rush, Edward T. Dibiana, and Claire P. Monks. 2017. Gendered penalties of divorce on remarriage in Nigeria: A qualitative study. *Journal of Comparative Family Studies* 48: 351–66. [CrossRef]
Longo, Mariano. 2015. *Fiction and Social Reality: Literature and Narrative as Sociological Resources*. Surrey: Ashgate Publishing Limited.
Magezi, Vhumani, and Christopher Magezi. 2017. A pastoral evaluation and responses to the challenge of spiritual insecurity in African pastoral ministry and Christianity. *Verbum et Ecclesia* 38: 1–13. [CrossRef]
Marx, Karl, and Friedrich Engel. 1967. *The Communist Manifesto*. London: Penguin Classics. First published in 1848.
Matza, David, and Gresham M. Sykes. 1961. Juvenile Delinquency and Subterranean Values. *American Sociological Review* 26: 712–19. [CrossRef]
Mauss, Marcel. 1925. *The Gift*. London: Routledge.
McGerty, Lisa Jane. 2000. "Nobody Lives Only in Cyberspace": Gendered Subjectivities and Domestic Use of the Internet. *Cyberpsychology, Behavior, and Social Networking* 3: 895–99. [CrossRef]
Melvin, Agunbiade Ojo, and Titilayo Ayotunde. 2010. Spirituality in Cybercrime (Yahoo-Yahoo) Activities among Youths in South West Nigeria. In *Youth Culture and Net Culture: Online Social Practices: Online Social Practices*. Hershey: IGI Global, pp. 357–76.
Morahan-Martin, Janet. 2000. Women and the Internet: Promise and Perils. *Cyberpsychology, Behavior, and Social Networking* 3: 683–91. [CrossRef]
Morris, Craig. 2018. 'You can't stand on a corner and talk about it . . . ': Medicinal cannabis use, impression management and the analytical status of interviews. *Methodological Innovations* 11: 1–12. [CrossRef]
Nkoh, Martius. 1963. *The Sorrow of Man*. Enugu: Okolue Books.
Ogwezzy, Michael Chukwujindu. 2012. Cyber crime and the proliferation of yahoo addicts in Nigeria. *International Journal of Juridical Sciences* 1: 86–102.
Okri, Ben. 1991. *The Famished Road*. London: Jonathan Cape.
Osoba, Segun O. 1996. Corruption in Nigeria: Historical perspectives. *Review of African Political Economy* 23: 371–86. [CrossRef]
Peavy, Daryl. 2016. The Benin Monarchy, Olokun and Iha Ominigbọn. *Journal of Benin and Edo Studies* 1: 95–127.
Peek, Philip M. 1991. *African Divination Systems: Ways of Knowing*. Washington, DC: Georgetown University Press.
Peek, Philip M. 2016. 'Twinning' and 'Perfect knowledge' in African Systems of Divination. In *Divination: Perspectives for a New Millennium*. Edited by Curry Pactrick. London: Routledge.
Powell, Anastasia, Gregory Stratton, and Robin Cameron. 2017. Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy* 6: 17–33.
Powell, Anastasia, Gregory Stratton, and Robin Cameron. 2018. *Digital Criminology: Crime and Justice in Digital Society*. New York: Routledge.
Reiner, Robert. 2016. *Crime, the Mystery of the Common-Sense Concept*. New York: John Wiley & Sons.
Rich, Timothy. 2018. You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal* 31: 1–18. [CrossRef]
Rock, Paul. 2005. Chronocentricism and British Criminology. *The British Journal of Sociology* 56: 473–91. [CrossRef] [PubMed]
Rosen, Norma. 1989. Chalk Iconography in Olokun Worship. *African Arts* 22: 44–53. [CrossRef]
Rush, Michael, and Suleman Ibrahim Lazarus. 2018. 'Troubling' Chastisement: A Comparative Historical Analysis of Child Punishment in Ghana and Ireland. *Sociological Research Online* 23: 177–96. [CrossRef]
Santa Ana, Otto. 2002. *Brown Tide Rising: Metaphors of Latinos in Contemporary American Public Discourse*. Austin: University of Texas Press.
Shankland. 1933. *Intelligent report on the Aro by T. M. Shankland*. CSO 26/29017. Ibadan: National Archives Ibadan, p. 13.
Smalls, James. 2015. The Science of Vodun, Vodoo: Professor James Smalls. [Online Video]. Available online: https://www.youtube.com/watch?v=6YkEPelFOKE (accessed on 5 December 2017).

Sogolo, Godwin S. 1991. The concept of cause in African thought. In *Philosophy from Africa: A Text with Readings*. Edited by Pieter Hendrik Cotzee and Abraham Pieter Jacob Roux. Oxford: Oxford University Press, pp. 177–85.

Stanislav, Andreski. 1996. *The African Predicament: A Study in the Pathology of Modernisation*. London: Michael Joseph. First published 1968.

Steinmüller, Hans. 2011. The moving boundaries of social heat: Gambling in rural China. *Journal of the Royal Anthropological Institute* 17: 263–80. [CrossRef]

Tade, Oludayo. 2013. A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs* 23: 689–705. [CrossRef]

Tankebe, Justice. 2008. Colonialism, legitimation, and policing in Ghana. *International Journal of Law, Crime and Justice* 36: 67–84. [CrossRef]

Thomas, William Isaac, and Dorothy Swaine Thomas. 1928. *The Child in America: Behaviour Problems and Programmes*. New York: Alfred Knopf.

Trend Micro and INTERPOL. 2017. Cybercrime in West Africa: Poised for an Underground Market. Available online: https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf (accessed on 7 July 2016).

Tyler, Tom. 1990. *Why People Obey the Law*. New Haven: Yale University Press.

Ujumadu, Vincent. 2015. Okija Shrine: No Longer a Bee-Hive of Activities for Politicians. Available online: https://www.vanguardngr.com/2015/08/okija-shrine-no-longer-a-bee-hive-of-activities-for-politicians/ (accessed on 20 November 2016).

US Consulate. 1949. *Records of the US Consulate, National Archives and Records Administration, Washington DC (NARA): Record Group 84, Classified General Records of the US Consulate and Embassy, Lagos, Nigeria, 1940–63, Box 1: C. Porter Kuykendall, Consul-General, to Secretary of State, May 16*; Washington, DC: NARA.

Washington, Teresa N. 2012. Mules and Men and Messiahs: Continuity in Yoruba Divination Verses and African American Folktales. *Journal of American Folklore* 125: 263–85. [CrossRef]

Weber, Max. 1992. *Economy and Society: An Outline of Interpretative Sociology*. Berkeley: California University Press. First published 1946.

Whitty, Monica, Matthew Edwards, Michael Levi, Claudia Peersman, Awais Rashid, Angela Sasse, Tom Sorell, and Gianluca Stringhini. 2017. Ethical and Social Challenges with developing Automated Methods to Detect and Warn potential victims of Mass-marketing Fraud (MMF). Paper presented at 26th International Conference on World Wide Web Companion, Perth, Australian, April 3–7; pp. 1311–14.

© 2019 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework

Suleman Lazarus

1. Introduction

This article sets out to discuss the value of feminist theory in understanding digital crimes. Almost a century ago, Freud (1927) had reminded us in his analysis of "civilisation and its discontents" that technology is not only responsible for our advancement, but also for our "misery" (see also Kirillova *et al.* 2017). It is indisputable that the critical aspects of costs and benefits associated with the use of information and communication technologies (ICTs) are different for men and women (Al Izki and Weir 2015; McGerty 2000; Mumporeze and Prieler 2017). Indeed, gender issues in cyberspace are reflections of their antecedents in society (Baym and boyd 2012; Braithwaite 2014; Jane 2016a,b); who is victimised, why, and to what effect are the critical starting points for the analysis of gender and crimes (Burgess-Proctor 2006; Cook 2016; Eagly 2016). However, these gender issues are obscured through the definitional lens of "cybercrime" and mainstream criminology theories. While mainstream criminologists have broadly taken for granted that men (and boys) predominate in traditional crimes as perpetrators, most generalisable criminological research on digital crimes is a mere reflection of the prevailing criminology theories of traditional crimes (Cook 2016; Potter 2015; Sharp 2015). This article is a plea for greater expansion of our analysis of gender issues in all areas of cyber criminology.

For Jaishankar (2007, 2011), "cyber criminology" is the notion that the causations, experiences, consequences, and patterns of crimes that are relevant in the physical space concurrently impact in the cyberspace and vice versa (see also Lazarus 2019; Powell *et al.* 2018). By the same token, in most investigations of crime, the polarisation of the real world and the virtual world obstructs the understanding of gender dynamics online (Braithwaite 2014; Eckert 2018; McGerty 2000; Morahan-Martin 2000a; Vasilescu *et al.* 2012). Indeed, "nobody lives only in cyberspace" (McGerty 2000, p.895). "Life online is a mere extension of life offline" since socially constructed cues on gender offline are concurrently impactful in the digital realm (Morahan-Martin 2000a, p.689). Using these ideas as a starting point, this paper asks: do structured gender relations retain their efficacy in online contexts? Do gender forces in society influence online behaviours and experiences? Doing so is prompted by two central motives: (a) to critique mainstream criminology and advocate the centrality of gender as a theoretical entry point for the investigating of all aspects of cyber criminology; (b) to critique the meaning of the term "cybercrime" and

Suleman Lazarus is an Austrian independent scholar who is currently a visiting lecturer at the University of Greenwich, United Kingdom. He is a qualitative sociologist and his research interests include the cultural dimensions of digital crimes. While he completed an empirical study on the connections between hip hop artists and cybercriminals in 2018, his conceptual work in 2019 nuances "the intersectionality of the spirit world and the acquisition of wealth." He is also a published poet and his most recent poem is entitled "Betrayals in academia and a black demon from Ephesus".
Email: suleman.lazarus@gmail.com

build a synergy between the feminist epistemology of crime and a conceptual cybercrime framework. The underlying impetus is that it is of the utmost importance for the umbrella term "cybercrime" and other typologies and theories that inhibit a more critical examination of gender dimension of crime to be revisited and redefined because they have significant consequences for interpretations. To illustrate that online behaviours and attitudes are mere extensions of offline social processes and relationships, this article will chronologically provide an overview of gender gaps in a range of digital crimes (online harassment, cyber-bullying, cyber-fraud, revenge porn, and cyber-stalking). It will also use a recent comparison of digital forms of crime including digital piracy, i.e., Donner's (2016) work, as a case study to illustrate how mainstream criminology (and the term cybercrime) has, for example, undermined the feminist epistemology of crime.

2. Theoretical guidance

2.1 Feminist criminology perspectives

One way to begin understanding feminist criminology is to examine how conceptions of gender and crime interact. Feminist criminology perspectives[1] or the feminist epistemology of crime advocate a more critical examination of gender issues regarding multiple social life experiences such as crime and justice (Braithwaite 1989; Burgess-Proctor 2006; Eagly 2016; Sabon 2016). Feminist criminology perspectives are not simply the study of crimes committed by women, nor are they just the study of women and crime (Naegler and Salman 2016; Sharp 2015). The feminist epistemology of crime explicitly takes into account the unequal power of boys/men and girls/women in its approach to the study of crime and gender (Lynch 2016; Naegler and Salman 2016). Many scholars have already noted that gender is situationally accomplished, socially constructed, and culturally performative, and its persistence as a significant factor in real-life experiences is remarkable (Agboola and Rabe 2018; Connell and Messerschmidt 2005; Mumporeze and Prieler 2017; Oakley 2018; Sabon 2016; Schiebinger 2000; West and Zimmerman 1987; Wood and Eagly 2010). Equally, this article, like many scholarly articles before it (e.g., Burgess-Proctor 2006; Dean and Platt 2016; Potter 2015), acknowledges that gender intersects with multiple axes of social (dis)advantages such as age, class, race, and sexuality: "[T]o advance an understanding of gender, crime, and justice, feminist criminologists must examine [these] linkages between inequality and crime using an intersectional theoretical framework" (Burgess-Proctor 2006, p.28). By the same token, feminist criminologists must examine these linkages in society that extend to cyberspace through the lens of digital intersectionality (Tynes, Schuschke and Noble 2016). Indeed, the multidisciplinary field of internet studies (e.g., cyber criminology, or digital criminology, computer-mediated communications, cyberpsychology) needs theoretical and methodological approaches that facilitate a more critical examination of the uneven power relations embedded in these intersections that exist in technological spaces (Jane 2016a; Tynes *et al.* 2016). However, while the article acknowledges that the lens of intersectionality is a significant paradigm in feminist scholarship, it admits that the intersections of the multiple categories involved are many and complex. This article, therefore, will mostly focus on gender and crime connections due to its limited scope. Equally, a core tenet of feminist criminology seeks "to expand criminological theorising about gender and to make gender a central theoretical starting point for theorising about crime" (Lynch 2016, p.3). In particular, "feminist criminology has been largely motivated by the acknowledgement that gendered analyses of crime are vitally important to the field and that sexism influences social life in ways that are nuanced, complex, and enduring" (Cook 2016, p.335).

Building on these ideas, this paper aims to contest the definitional rigidity of the umbrella term (i.e., cybercrime). In a similar vein to feminist criminology, mutually constitutive categories shape people's identities, experiences, and perceptions of all aspects of life, both tangible and intangible (Lynch 2016; Sabon 2016; Schiebinger 2000). Both offenders and victims possess some commonalities, and one of the most salient of these is gender (Hutchings and Chua 2017; Watts *et al.* 2017). Arguably, as McGerty (2000), Eklund (2011), Lazarus (2019), and Vasilescu *et al.* (2012) pointed out, offline and online contexts are not separate entities with a clearly defined boundary, because people can never be online without being offline too. For example, gender practices and patterns in society continue to thrive in new media (Baym and boyd 2012),

© 2019 John Wiley & Sons Ltd

whereas "online abuse of women is not fully recognised as entangling online and offline communications" (Eckert 2018, p.1282). Examining gender differences in the virtual world prompts one to consider how cultural nuances inhibit and promote behaviour that, in turn, could shape a person's criminal or law-abiding social actions (Flavin 2001; Jane 2016a; Lazarus and Okolorie 2019). Arguably, examining the gender disparities in cybercrime types is crucial to critiquing mainstream criminology theories as well as the term "cybercrime".

2.2 Feminist critique of mainstream criminology

Mainstream criminological theories claim to offer generalisable explanations of criminal offending, whereas they have, to a large extent, taken for granted the predominance of men (and boys) in offending (Cook 2016; Daly and Chesney-Lind 1988; Potter 2015). This is because most researchers follow theory as believers follow theology (Rimer 1997). Similarly, according to feminist criminology perspectives, most mainstream criminology theories[2] have missed critical opportunities necessary to advance our understanding of gender and crime (Cook 2016; hooks [1984] 2000; Sharp 2015). Prominent among these theories is "A General Theory of Crime", which argues that, while low self-control has a direct and causal link to all offending, "men are always and everywhere more likely than women to commit criminal acts" (Gottfredson and Hirschi 1990, p.143). The rationale for using this theory as an example acknowledges its substantial influence in criminology and related disciplines. Indeed, as Cook (2016) observed, it has attracted enormous central funding for doctoral training and consequently served as critical theoretical guidance for many doctoral projects in criminology. In particular, according to Cook's (2016) assessment, A General Theory of Crime is closely associated with over 177,000 academic published articles and 57 books. It has not only inspired many academic publications, but it has also extended the conception of crimes beyond the legalistic definition to include "acts of force or fraud undertaken in pursuit of pleasure" (Gottfredson and Hirschi 1990, p.15), which is one of its fundamental contributions.

However, by failing to closely examine gender as an analytical framework, it has ignored gender as a critical source of social (dis)advantage,[3] which influences patterns of crime and victimhood (Braithwaite 1989; Potter 2015). As Geis (2000, p.40) rightly asked: "how can the general theory of crime incorporate the uncounted number of criminal abortions undergone by women before *Roe v. Wade* in 1973 legalised the procedure?" Indeed, it would be a stretch to maintain that the presence of low self-control explains the actions of women who have opted for illegal abortions (Geis 2000). Debatably, Gottfredson and Hirschi (1990) failed to see that self-control contains "unacknowledged value assumptions" (Geis 2000) and involves socioeconomic and cultural dynamics (Potter 2015). For example, research in many nations, such as Puerto Rico (Maldonado-Molina *et al.* 2009), Japan (Chen *et al.* 2010), Ghana (Boakye 2013), Korea (Bae 2017), and Nigeria (Ibrahim 2017), illustrates that this is so. These authors highlight that self-control is not immune to socio-cultural assumptions and socially constructed cues (e.g., gender nuances), which vary across cultures.

To ignore socially constructed cues such as gendered nuances not only undermines the centrality of these nuances as conceptual entry points for examining crimes but has enduring real-life consequences in academia. For example, as Sharp (2015, p.912) succinctly noted, "generations after generations of students are unaware of feminist criminology and its contributions. They in turn teach their own students mainstream theories, with little, if any, reflection on more explicitly feminist approaches". It is also conceivable that these "generations after generations of students" would use mainstream theories to examine new forms of crimes in digitalised societies (digital crimes) at the expense of the feminist epistemology of crime. Arguably, mainstream criminology theories (e.g., A General Theory of Crime) and their generational subscribers not only perpetuate androcentric conceptions within criminology (Potter 2015), but they dismiss volumes of criminological research documenting that gender is a crucial index factor in crime and victimisation (Cook 2016; Eagly 2016).

In a nutshell, most mainstream criminology theories (e.g., A General Theory of Crime) have missed critical opportunities necessary to advance our understanding of gender and crime (Cook 2016; hooks [1984] 2000; Sharp 2015). That is, the real world and the virtual one are not independent spaces

© 2019 John Wiley & Sons Ltd

and internet users are rooted in both worlds simultaneously (Braithwaite 2014; Eckert 2018; Eklund 2011; Vasilescu *et al.* 2012). To draw attention to these issues would encourage rather than discourage "corporations and governments agencies in addressing misogyny issues in the cyberspace" (Jane 2016a, p.292). Therefore, this paper is a theoretical endeavour that explores the synergy between feminist criminology and a conceptual cybercrime framework to argue for the centrality of gender as a conceptual starting point for investigating the socioeconomic and psychosocial impacts of ICTs. The underlying impetus is that most mainstream criminological theories sidetrack gender nuances and impose their mainstream image upon the feminist epistemology of crime. Equally, most generalisable cybercrime typologies limit the windows of opportunity to examine gender differences concerning a range of digital crimes and their motivations. This current paper sets out to move gender analysis of digital crimes, in hooks' ([1984] 2000) term, "from margin to centre".

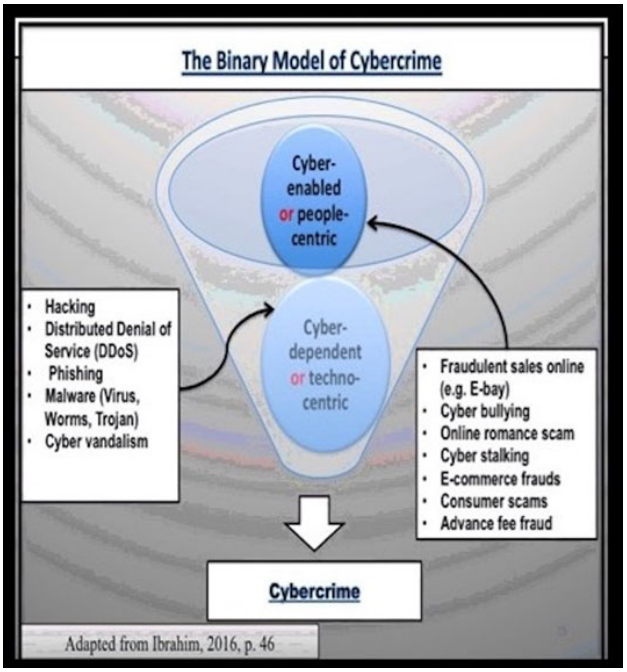


FIGURE 1. The cybercrime dichotomy [Colour figure can be viewed at wileyonlinelibrary.com]

3. The meaning of cybercrime and ambiguities

3.1 An umbrella term and dual typologies

Cybercrime refers to any criminal activity carried out through the use of ICTs and the internet (e.g., Gordon and Ford 2006; Richardson and Gilmour 2015). It has been defined in different jurisdictions and by many scholars (e.g., Gordon and Ford 2006; Hutchings and Chua 2017) and security agencies (e.g., National Crime Agency 2017; Norton 2015) to mean slightly different things. However, the most consistent idea is that the term "cybercrime" is an umbrella word for a wide spectrum of digital crimes such as hacking, cyber espionage, cyber-stalking, cyber fraud, cyber vandalism, online revenge pornography, and the distribution of computer viruses (Donner *et al.* 2015; Ibrahim 2016; Kirillova *et al.* 2017; Yar 2017). The term "cybercrime", on the one hand, is overly broad, and on the other it is rigid. By implication, it is resistant to change because it is "loosely" used in everyday parlance as a simple "acronym" for all forms of crimes on the internet. Consequently, there is a fairly clear pattern to suggest that in using the term "cybercrime" as a given, multitudes of researchers "clump together" a wide spectrum of digital crimes with arbitrary attributes (e.g., Bidgoli and Grossklags 2016; Hill and Marion 2016; Sabillon *et al.* 2016). This paper attempts to highlight the analytic consequences of this homogenisation on gender issues. Many other scholars (e.g., Gordon and Ford 2006; McGuire and Dowling 2013; Rokven *et al.* 2018) have used the terms "cyber-enabled crimes", "people-centric cybercrimes" or "cyber-dependent crimes" to represent a range of crimes, regardless of the ambiguity the terms embody. As illustrated in Figure 1, cyber-enabled crimes or people-centric cybercrimes encompass all crimes that existed before the advent of ICTs and that can now be digitalised, whereas cyber-dependent crimes or techno-centric cybercrime comprise crimes or behaviours that were made possible through the development of ICTs.

The cyber-enabled/people-centric category encompasses a broad spectrum of digital crimes with arbitrary attributes, where they obscure the meaning of each cybercrime type they represent, which is problematic (Ibrahim 2016). Cyber-enabled or people-centric cybercrime includes a wide variety of criminal activities ranging from

© 2019 John Wiley & Sons Ltd

the illegal downloading of music (digital piracy) to revenge pornography. Indeed, many of the digital crimes that some researchers (Gordon and Ford 2006; McGuire and Dowling 2013) forced under one rubric (i.e., cyber-enabled or people-centric) appear distinctive enough to require other kinds of explanations if we expect to be able to understand them, their effects, and their occurrence with some degree of consistency – other than that they are "cyber-enabled".

For example, cyberbullying and fraudulent sales on eBay involve different motivations, victim–perpetrator gains/losses and victim–perpetrator relationship/dynamics, as shown in Table 1 (for a fuller critique of varying cybercrime classifications, see Ibrahim 2016). This article builds on Ibrahim's (2016) idea that social/contextual factors apply online as they do offline and aims to advance it by explicitly taking into account the perspectives of feminist criminology. Accordingly, given that such crimes (i.e., cyberbullying and fraudulent sales on eBay) are qualitatively different, this current endeavour sets out to highlight that these umbrella terms (e.g., cybercrime or cyber-enabled crimes) have, by implication, debilitated the examination of gender comparison between cyberbullying and fraudulent activities. As regards cyberbullying and cyber-fraud, the victim–perpetrator motives and gains and losses are not the same, as shown in Table 1. In other words, the homogenisation of crimes with different core attributes not only inhibits the policing of these crimes (Rosenbach and Belk 2012) but also debilitates a more critical examination of gender psychology and victimisations in a wide spectrum of digital crimes.

Indeed, online behaviours and attitudes are extensions of offline social processes and relationships (Al Izki and Weir 2015; Citron 2014; Lazarus 2019). Empirical evidence from many cultures[4] such as Sweden (Priebe and Svedin 2012), Rwanda (Mumporeze and Prieler 2017), Australia (Hutchings and Chua 2017), Nigeria (Lazarus 2018), Thailand (Ojanen *et al.* 2015), Canada (Cunningham *et al.* 2015), Korea (Bae 2017), Germany, Switzerland, the United Kingdom, and the United States (Eckert 2018) demonstrate that this is so. "Differences between men's and women's experiences of the internet are linked to broader questions of gender in society, and therefore gender issues in cyberspace are likely to persist as long as they exist offline" (Sherman *et al.* 2000, p.893; see also Jane 2016a; Eckert 2018). Anchoring on the above insights, while "understanding gender inevitably involves comparisons, such comparisons are essential to developing an understanding of the psychology of gender" (Eagly 2016, p.286) and victimisations. Conceptually, this paper sets out to advocate the centrality of gender as a starting point for investigating various types of digital crimes.

3.2 The Tripartite Cybercrime Framework (TCF)

Social and contextual factors are a resource for understanding the connections between gender and digital crimes (Citron 2014; Jane 2016a; Lazarus and Okolorie 2019). A nascent typology, and one better suited to investigating the linkages between gender and digital crimes, is the Tripartite Cybercrime Framework (TCF) proposed by Ibrahim (2016). According to the TCF, cybercrime can be divided into three broad motivational parts: socioeconomic; psychosocial; and geopolitical. Socioeconomic cybercrime can be defined as the computer- and/or internet-mediated acquisition of financial benefits by false pretence, impersonation, counterfeiting, forgery, or any other fraudulent representation of facts such as online fraud, credit card fraud, romance scams, and e-embezzlement.

Psychosocial cybercrime refers to digital crimes that are primarily psychologically driven, such as cyber-stalking, cyberbullying, and cyber-harassment, whereas geopolitical cybercrimes can be defined as those cybercrimes that are fundamentally political in nature and involve agents of the state and/or industrial representatives, e.g., cyber espionage. The TCF is more robust than the term "cybercrime" and other classifications mentioned in Figure 1 in dealing with the complexities of numerous varieties of cybercrime types. Because structured gender relations retain their efficacy in online contexts, this research will particularly benefit from the TCF. The lens of binary classifications and that of the buzzword "cybercrime" (discussed above) are ill-equipped, for example, to differentiate between the psychosocial and socioeconomic categories. Unlike these classifications (e.g., the dual groups), the TCF acknowledges the importance of different motivations behind criminal behaviours. These characteristics in themselves bring the TCF closer to the feminist

© 2019 John Wiley & Sons Ltd

TABLE 1. Perpetrators' benefit and victims' losses

PERPETRATOR & VICTIM	*SOCIOECONOMIC*	*PSYCHOSOCIAL*	*GEOPOLITICAL*
Perpetrator (primary benefit)	Economic gain	Psychological gain	Geopolitical, psychological & economic gain
Victim (primary loss)	Economic loss	Psychological loss	Geopolitical, psychological & economic loss
Perpetrator (secondary benefit)	Psychological gain	Economic gain	Geopolitical, psychological & economic gain
Victim (secondary loss)	Psychological loss	Economic loss	Geopolitical, psychological & economic gain

epistemology of crime than other typologies mentioned.

3.3 The Tripartite Cybercrime Framework (TCF) and feminist criminology connections

There is an implicit overlap between the TCF and the feminist epistemology of crime. The TCF is rooted in social and cultural nuances of crime and victimisation. It is essentially based on the premise that perpetrators and victims of a wide spectrum of digital crimes have a unique relationship and that this relationship is fundamentally based on the perpetrators' primary motivations and benefits and the victims' primary losses, as mentioned and shown in Table 1 (adapted from Ibrahim 2016, p.47). Given that, for example, online abuse disproportionately affects women (e.g., Citron 2014) and "online abuse of women is not fully recognised as entangling online and offline communication" (Eckert 2018, p.1282), conceptually, the TCF offers avenues to situate gender at the core of crime analysis. Theoretically, locating gender at the core of crime investigation acknowledges the sources of social advantage and disadvantage in society. While sources of social advantage and disadvantage are related to patterns of offending and victimisation (Näsi *et al.* 2015; Newburn 2016), gender is one of the critical sources of social advantage and disadvantage in society (Fogiel-Bijaoui 2016; Lavee and Benjamin 2017; Lazarus *el al.* 2017; Tynes *et al.* 2016). For example, unlike men, deprived Israeli mothers are forced to pay rents in the coin of sexual services (Lavee and Benjamin 2017). On the flipside, women's possession of high economic power can have detrimental effects on their marriages and their chances of remarriage in Nigeria (Lazarus *et al.* 2017).

The critical point here is that gender inequality itself structures these types of women's experiences in Israel and Nigeria mentioned above. Indeed, gender is a central source of social disadvantages that positions these women between exclusion and belonging. Relatedly, for the TCF, it is conceivable that gender comprises the everyday reality of crime and victimisation, especially the perpetrator–victim gains and losses. Similarly, for the feminist epistemology of crime, the analysis of gender and crime begins with understanding who become victims and why and what results ensue (Cook 2016; Eagly 2016; Potter 2015). For example, focusing primarily on cyber-hate, Jane (2016b, p.10) observed that "women are being attacked online more often, more severely, and in far more violently sexualised ways than men" (see also Eckert 2018). The mismatch between men's and women's involvement in, and experiences of, internet crime are linked to broader questions of gender in society (Citron 2014; Hutchings and Chua 2017).

Additionally, for feminist perspectives, contextual lenses are invaluable tools of analysis. For example, Jones' (2018) analysis of international interoperability outlined the long histories of the different cultural and legal contexts involving many nations, e.g., European countries and the United States. Similarly, for the TCF, "jurisdictional cultures and nuances apply online as they do offline" (Ibrahim 2016, p.44). Indeed, while the TCF takes into account the cultural and contextual nuances of crime, it acknowledges the importance of the motivation-based relationship between offenders and victims in its classification of cybercrime. Relatedly, feminist criminology explicitly takes into account the unequal power of boys/men and girls/women in its approach to the study of crime and justice.

© 2019 John Wiley & Sons Ltd

3.4 Contrasting the socioeconomic and psychosocial cybercrimes types

This current endeavour operationalises this framework (TCF), which comprises three components. However, it focuses on only two parts (i.e., the socioeconomic and psychosocial cybercrime groups) to contrast the nature of their attributes. This strategy resonates with the view that the motivations, victimisations, and relational processes involved in these two parts are more connected with the broader online experiences of individuals than that of the geopolitical category (e.g., cyber espionage) (Ibrahim 2016). While the distinctions between these groups are remarkable (as illustrated in Table 1), the TCF is based on the premise that "the perceived world comes as structured information rather than as arbitrary attributes, [and], this condition can be achieved either by the mapping of categories to given attribute structures or by the definition or redefinition of attributes to render a given set of categories appropriately structured" (Rosch 1978, p.28; see also Ibrahim 2016, p.45). For example, there is a reasonably clear pattern that victims of psychosocial cybercrimes such as revenge porn, cyber-harassment, cyber-hate, and cyberbullying, directly and primarily experience a range of similar emotional, psychological, and behavioural health consequences. These consequences include anxiety, self-harm, depression, low self-esteem, and suicidal ideation to varying degrees (Jane 2016b; Watts *et al.* 2017). However, in addition to the direct psychological costs of psychosocial cybercrimes, coping with these psychologically-based crimes can have indirect financial consequences. For example, costs associated with therapy, residential mobility, and time taken off work can drain a victim's financial resources. The same primary and secondary losses do not fit squarely with victims of cyber-fraud (socioeconomic cybercrime), as illustrated in Table 1.

Some researchers (e.g., Tan and David 2017; Whitty and Buchanan 2012, 2016) also suggest that the act of deception involved in fraud can be driven by a non-monetary reward such as a "psychological thrill". Equally, they argue that a financial loss due to cyber-fraud can manifest in the victim physiologically as distress. These researchers (e.g., Whitty and Buchanan 2016) mainly investigated the experience of romance-scam victims. In romance scams, "criminals pretend to initiate a relationship through online dating sites then defraud their victims of large sums of money" (Whitty and Buchanan 2012, p.181). Thus, their finding regarding the negative psychological consequences for victims may be particularly marked given that romance scams are in the realm of love and friendship and may not be reflective of the experiences of victims of other forms of cyber-fraud (e.g., insurance fraud, and the misappropriation of public funds) without the romance component. As Button and Cross (2017) and Schoepfer *et al.* (2017) noted, cyber-fraud includes hybrid fraudulent acts such as credit card scam, identity theft, intellectual property crimes, financial/bank fraud, and romance scams. Hence, undoubtedly and primarily, a strong motivation for cyber-fraud and a direct primary loss due to cyber-fraud is money, as shown in Table 1. By implication, cyber-fraud is rooted in socioeconomics. Even though victims are in some cases spiritually manipulated, the spiritual/magical manipulations of victims are rooted in socioeconomics (Lazarus 2019; Lazarus and Okolorie 2019). But the same cannot be said regarding psychosocial cybercrimes such as revenge porn and cyberbullying, which are fundamentally more expressive or relational than socioeconomic cybercrimes. For example, while the negative experiences of women bloggers (e.g. cyber-stalking, cyber-bullying, and rape threats), discussed in Eckert's (2018) article, cannot be described as being primarily rooted in socioeconomics, indisputably, they belong to the psychosocial classification.

It is thus reasonable to suggest that psychosocial cybercrimes such as cyberbullying manifest more through relational processes than socioeconomic cybercrimes such as cyber-fraud. It is also reasonable to agree that the TCF fits with the psychology of gender perceptions and victimisations of crime because the sources of social advantage and disadvantage apply online as they do offline. In fact, "power is not distributed equally online, and this in itself may increase rather than decrease prevailing gender differences in society" (Morahan-Martin 2000a, p.683; see also Eckert 2018). In turn, this article acknowledges here that gender is critical to the analysis of socioeconomic and psychosocial cybercrime categories (with distinctive perpetrator/victim gains and losses mentioned), and this in itself underscores the utilitarian value of the TCF alongside feminist criminology perspectives. Henceforth, this current effort explores the synergy

© 2019 John Wiley & Sons Ltd

TABLE 2. Operational definitions of the six cybercrime types outlined

Cybercrime Types	*Category*	*Operational Definition*	*Authors*
Online harassment	Psychosocial	Online harassment can be defined as the act of aggressively pressuring, intimidating, distressing or spread denigrating rumours about others.	Everbach (2018, p.134)
Cyberbullying	Psychosocial	Bullying is an intentional, aggressive behavior, carried out repeatedly against a victim, whereas with cyberbullying, the power imbalance between bully and victim and the repetitiveness of the behavior typically involved in traditional bullying are often missing from the equation.	Cartwright (2016, p.2)
Cyber-fraud	Socioeconomic	Cyber-fraud refers to the computer or/and internet-mediated acquisition of financial benefits by false pretence, impersonation, manipulation, counterfeiting, forgery or any other fraudulent representation of facts.	Ibrahim (2016, p.48)
Revenge porn	Psychosocial	Revenge porn is defined as non-consensual sharing of sexually explicit images (including photographs) and/or videos, with an underlying motivation linked to revenge.	Walker and Sleath (2017, p.2)
Cyberstalking	Psychosocial	Cyberstalking or "cyber dating abuse" can be defined as the use of the internet and other technological devices to monitor or harass another person in a threatening way.	Marcum et al. (2017, p.375)
Digital piracy	Socioeconomic	While digital piracy involves the illegal uploading or downloading of computer files and software, offenders generally victimise creative artists, and their respective industries, whose creative works they acquire without paying for them.	Donner (2016, p.558)

between the feminist perspective and two parts of the TCF to illustrate that while conceptions of gender and crime interact, they also intersect with other categories (e.g., culture and sexuality) to provide additional layers of explanation. In order to achieve this, article pays particular attention to six online crimes[5] (outlined in Table 2).

4. Overview of gender gap online

4.1 Gendering online harassment (psychosocial category)

While a person's gender is a product of social constructions, it has real-life consequences (Cook 2016; Everbach 2018; Naegler and Salman 2016) that manifest in the virtual as they do in the real world. The manifestations of these real-life repercussions of gender are less obscured if people's perceptions of digital crimes are framed with the TCF alongside feminist criminology perspectives than with the term "cybercrime" and the binary typologies. The underlying idea is that the motivations, victimisations, and relational processes involved in digital crimes listed in Table 2 do not commonly situate women and men similarly. For example, as regards online harassment (psychosocial cybercrime), Lindsay and Krysik's (2012) survey of 342 university students and Finn's (2004) survey of 339 college students support the above assertion regarding the importance of factoring gender into the cybercrime equation. Their studies (both in the United States) found that the perpetrator–victim relational processes were particularly apparent in online harassment because

© 2019 John Wiley & Sons Ltd

the majority of participants reported that the perpetrators were people known to the victims. Regarding the gender gap in online harassment, Barlett and Coyne's (2014) meta-analysis of 109 studies found that while boys are more likely than girls to commit online harassment in general, girls were more likely to engage in cyber-harassment during adolescence in particular. The underlying assumption is that adolescence in itself is a time of turmoil[6] (Hazen *et al.* 2008; Larsen and Ham 1993; Schneider and Csikszentmihalyi 2017) and adolescent children, irrespective of their gender, commonly report more negative conflict with their parents and peers.

However, a few studies, such as those of Marcum *et al.* (2012) and Holt *et al.* (2012), suggest that women are more likely than men to harass their peers online. While the above findings indicate that it is unclear whether there are consistent gender trends in online harassment, none of the studies enquired as to whether online harassment (psychosocial cybercrime) is more gendered than socioeconomic cybercrimes, such as cyber-fraud, given the differences between them discussed above. Closely related to online harassment is cyber-bullying. Clear distinctions between cyber-bullying and online harassment (as far as perpetrators and victims are concerned) have not yet been thoroughly made in psychology (Englander *et al.* 2017). Nonetheless, unlike cyber-bullying, online harassment typically lacks a perpetrator–victim power-imbalance structure (Englander *et al.* 2017).

4.2 Gendering cyberbullying (psychosocial category)

Most generalisable research on gender gaps in bullying suggests that boys/men are more likely to be involved in physical bullying (e.g., Beckman *et al.* 2013; Berger 2007; Smith 2012), whereas girls/women are more involved in verbal, expressive, and relational bullying (e.g., Beckman *et al.* 2013; Berger 2007). The meta-analysis by Watts *et al.* (2017) of 54 published articles highlighted that individuals' gender is implicated in leading them to become cyber-bullies or continue to be victims. In a similar vein, various studies of students (Aricak 2009; Cunningham *et al.* 2015; Kraft and Wang 2010; Schenk and Fremouw 2012) have found that while women were more likely to report involvement as cyber-bullying witnesses, men were more likely to report involvement as perpetrators. Consistent with the above studies, Boulton *et al.*'s (2012) study of 405 undergraduates in the United Kingdom indicated that women view cyber-bullying, and those who perpetrate it, more negatively than their counterparts (men). Relatedly, Faucher *et al.*'s (2014) survey of 1925 Canadian university students reported that fewer men than women were cyber-bullied by acquaintances and friends.

However, while the above studies portray a fairly clear pattern regarding gender trends in cyber-bullying, they relied exclusively on university students for their studies' samples, and this pattern of data may have influenced the authors' assertions. Their assertions may not be generalisable to other populations, primarily because how researchers produce knowledge is relevant to what the claims are. Youth cultures and the exaggerated masculinity inherent in youth groups may have shaped the pattern of their results. Additionally, as some researchers (Donner 2016; James 2010) have observed, while it may be unclear whether there are consistent gender trends in cyber-bullying, the more diffused lifestyles available in cyberspace complicate any gender trends within bullying in the virtual world. "Indeed, greater computer expertise may resolve the power imbalance associated with traditional bullying, conferring greater power unto those who might otherwise lose a schoolyard fight or a 'real world' popularity contest" (Cartwright 2016, p.2). While considerations of the higher computer expertise of a victim may or may not change the status quo typically associated with gender trends in traditional bullying, none of the above studies probed whether psychosocial cybercrimes such as cyber-bullying are more gendered than socioeconomic cybercrimes, such as cyber-fraud, given their dissimilarities through the lens of the TCF, mentioned earlier.

4.3 Gendering cyber-fraud (socioeconomic category)

Regarding cyber-fraud, general populations most ordinarily view fraud by any means (online and offline), and by both juvenile and adults, as similarly reprehensible (e.g., Schoepfer *et al.* 2017). Insights from white-collar crime suggest that most women who embezzled money excuse their fraudulent behaviour through feminine themes (e.g., caregiver

© 2019 John Wiley & Sons Ltd

role), whereas by contrast most men who embezzled account for their crime through masculine themes, reflecting gender roles and nuances in society (e.g., Zietz 1981). Similarly, Klenowski *et al.* (2011), who interviewed 40 inmates in the United States, examined how men and women "do gender" when accounting for their crimes in their interview study. They found that offenders draw on gendered themes to align their actions with cultural expectations of masculinity and femininity. For example, qualitative studies found that while Nigerian[7] men (and boys) predominate in "cybercrime" as perpetrators, most Nigerians involved in "cybercrime" types, in general, are involved in cyber-fraud in particular (e.g., Aransiola and Asindemade 2011; Lazarus 2018; Lazarus and Okolorie 2019). Women, however, play subordinate roles, such as the retrieval of fraud proceeds (e.g., Jegede *et al.* 2016; Lazarus and Okolorie 2019). Ibrahim (2017), who interviewed 17 parents, demonstrated that gender roles involved in cyber-fraud perpetration are reflective of a complex web of familial factors and cultural forces.

Familial and cultural forces socialise men and women as masculine and feminine individuals (Oakley 2018). Cultural expectations of masculinity and femininity perpetuate the domination of men over women (Connell and Messerschmidt 2005, p.832) and in Nigeria, men (and boys) are socialised to be sole bread-winners and the principal head of the household (Ibrahim, 2015; Smith, 2017). Under customary and Islamic types of marriages, some men can marry multiple wives[8] (Lazarus *et al.* 2017), which increases their financial responsibilities: "In virtually every arena of Nigerian men's lives, money's value is closely tied to the social work that it does in men's relationships with women" (Smith 2017, p. 160). Since gender category membership is attached to the cultural expectations and performativity (Connell and Messerschmidt 2005; West and Zimmerman 1987), in this context, "men's cultural positionality in society influences them to be generally more 'desperate' to achieve financial success than women online"–cyber-fraud (Ibrahim 2016, p.54).

Based on the preceding insights, I argue that men's hegemonic role in cyber-fraud as perpetrators is the mirror of, and made possible by, women's subordinate position in society. Additionally, I argue that, for many Nigerian cyber-fraudsters, cyber-fraud is a way of demonstrating their masculinity when legitimate means are denied. The critical point here is that cultural factors in Nigeria intersect with gender and cyber-fraud. Through the lens of intersectionality, the value of a cultural context becomes more apparent. While the Nigerian culture, for example, serves as a resource for understanding gender and crime connections, it offers additional layers of explanation.

How such cultural contexts can be used as a resource for understanding gender and crime connections is also exemplified in the connection between music and cyber-fraud. Weitzer and Kubrin's (2009) analysis of rap songs in the United States showed that while masculinity and femininity are central themes in music, artists do not work in a vacuum, and their songs are reflective of the broader gender hierarchy in society (see also Efthymiou and Stavrakakis's 2018 analysis of gender and music in Greece). Similarly, Lazarus's (2018) study, which examined the ways Nigerian cyber-fraudsters are represented in hip-hop music, is revealing (see also Lazarus and Okolorie's 2019 study, which interviewed 40 Nigerian law enforcement officers). These studies (Lazarus 2018; Lazarus and Okolorie 2019) found that while some musicians and cyber-fraudsters are "birds of a feather that flock together", the core aspects of their relationship are based on reciprocal economic benefits and determined by them. "Some musicians are convicted cyber-fraudsters or ex-cyber criminals, and some others are beneficiaries of active cybercriminals' fraudulent activities" (Lazarus 2018, p.71). Of interest is the observation that "fewer women than men glamorised cyber-fraud and cyber-fraudsters in their songs" (p.73). The link between cyber-fraud and music reinforces that online and offline lives are inextricably intertwined. In turn, real bodies and real people are affected[9] not only according to their gender but also through the prisms of popular culture, which acknowledges the importance of Tynes *et al.*'s (2016) notion of the digital intersectionality. This article, however, pays more attention to gender and crime connections than other categories, as previously mentioned.

While the above discussions expose the intersectionality of gender, the socioeconomic cybercrime (i.e., cyber-fraud), familial factors and popular culture, gender may be more of an index factor for victimisation in psychosocial cybercrimes than socioeconomic cybercrimes. For example, in light of the broader experience of fraudulent activities

© 2019 John Wiley & Sons Ltd

(e.g., in the context of online shopping) in people's lives, socioeconomic victimisations are different from those that are psychosocial, since a majority of people, irrespective of their gender, regularly experience fraudulent sales online (e.g., eBay) (FBI 2010, 2016). Unlike psychosocial cybercrimes, socioeconomic digital crimes are primarily financially motivated victimisations. Equally, this resonates with the view that the primary and secondary consequences of socioeconomic and psychosocial victimisations are qualitatively different, as shown in Table 1 (which challenges the definition of the umbrella term, "cybercrime"). While relational processes and dynamics mainly separate socioeconomic cybercrimes (e.g., credit card fraud and digital piracy) from psychosocial digital crimes (e.g., cyber-bullying and revenge porn), the latter is more expressive than the former.

4.4 Gendering revenge porn (psychosocial category)

Concerning revenge porn, a summary of the current state of knowledge comes from Walker and Sleath's (2017) review of 82 published studies.[10] They reported that while four studies, which examined the gender gap among adult populations, explicitly stated that the victimisation rates were higher for men than women, the gender gap was statistically significant in only a few studies (e.g., Priebe and Svedin 2012) (for a fuller analysis, see Walker and Sleath 2017). A careful examination of Priebe and Svedin's (2012) study in Sweden (involving 1,592 men and 1,840 women) perhaps sheds further light on the meaning of the gender gap in question. These authors argue that cultural nuances have double standards for men and women sexual minorities (e.g., homosexual and bisexual), which might have affected the above findings on any gender gap. These researchers (e.g., Priebe and Svedin 2012) revealed that a sexual minority group of men had almost sixfold increased odds of victimisation, whereas for women the increased odds were only twofold compared to their heterosexual counterparts.

Gender and sexuality could be seen as two sides of the same coin: they mutually construct each other. Indeed, sexuality intersects with gender and crime victimisation to offer a deeper explanation. While the legal and cultural contexts of nation states undeniably shape how the experiences of victims vary (Jones 2018), these contexts are critical to our understanding of who is victimised, why, and to what effect. For example, the Nordic nations (e.g., Finland and Sweden) and West African countries (e.g., Ghana and Nigeria) are almost at the opposite ends of the spectrum as far as the social rights of minorities, in general, are concerned (Ibrahim and Komulainen 2016; Rush and Lazarus 2018). The legal and cultural penalties of homosexuality in Sweden are far less severe than those in Nigeria, where, for example, homosexuality can lead to capital punishment in the northern region and 14 years' imprisonment in the southern region (Adebanjo 2015). While the lens of intersectionality provides additional layers of explanation, it also resonates with Buist and Lenning's (2016), Cook's (2016) and Ball *et al.*'s (2018) view that placing non-binary gender nuances as a theoretical starting point for investigating crimes would stimulate a more productive and more complete criminology awakening from slumber.

In this respect, Drouin *et al.*'s (2013) study on revenge porn in the United States elaborated that victimisation, in general, was most prevalent, in ascending order of significance, among people in committed relationships (3 per cent), "no strings attached" relationships (15 per cent), or cheating relationships (21 per cent). Based on this evidence, it is conceivable that mainstream cultural norms and values about gender roles and "good" sexual relationships are influential in shaping both the patterns and extent of victimisations. Nonetheless, while the above studies about gender gaps examined revenge porn, none compared psychosocial (e.g., revenge porn) and socioeconomic categories (e.g., cyber-fraud and illegal downloading of items). This conceptual article therefore aims to encourage researchers to investigate whether gender is more of an index factor for psychosocial cybercrimes than those which are socioeconomic (in line with the TCF and feminist criminology).

4.5 Gendering cyberstalking (psychosocial category)

While people perceive stalking through any means (online and offline) as similarly severe (e.g., Garnett-Bower 2017), some researchers have assumed that the men-perpetrator/women-victim structure applies as equally to cyber-stalking as it does to physical stalking (e.g., Purcell *et al.*

© 2019 John Wiley & Sons Ltd

2009). However, like cyber-bullying, other central premises are far from straightforward. Notably, Smoker and March (2017) suggested that the boundary between men and women in participating in and experiencing cyber-stalking behaviour is blurred. Some researchers (e.g., Helsper and Whitty 2010; Purcell *et al.* 2001, 2010) found that women were more likely than men to cyber-stalk their partners covertly. In particular, Helsper and Whitty (2010) surveyed 920 people in the United Kingdom and found that married women were more likely than men to use technology to monitor their partner's behaviour discreetly.

The above researchers (Helsper and Whitty 2010; Purcell *et al.* 2010) suggest that women (more so than men) use technology as a monitoring "toolbox" to maintain committed relationships. In a similar vein, Smoker and March (2017, p.393) concede: "the motivation to attain intimacy through preserving or establishing a relationship may provide women with the drive to conduct IPCS [increased opportunities for intimate partner cyber-stalking]". On the flipside, Marcum *et al.* (2017) surveyed 890 university students and highlighted that men were more likely to cyber-stalk and attempt log-ins to their partner's social media accounts. Marcum *et al.* (2017) explained the men-perpetrator/women-victim structure as implicitly constituting "cyber dating abuse", whereas other researchers (e.g., Helsper and Whitty 2010; Purcell *et al.* 2001) framed their findings slightly differently, as discussed above.

A closer consideration suggests that Helsper and Whitty (2010) surveyed people primarily over 30 years old (in the United Kingdom), whereas Marcum *et al.* (2017) surveyed youths under 30 years old (in the United States). If the above findings (Helsper and Whitty 2010; Marcum *et al.* 2017) are taken as a given, it is conceivable that gender roles and cultural obligations in society (e.g., feminine roles and the social obligations of a married woman to protect her committed relationship delicately) shaped their perceptions and behaviours regarding cyber-stalking. The bottom line here is that age interacts with gender to provide an additional layer of explanation, which acknowledges the value of the lens of intersectionality. Equally, even though the legal and cultural contexts in the United States and the United Kingdom about cyber-stalking vary (Jones 2018), it is reasonable, however, to argue that gender and cultural commitments in the nations where these studies were based offer central explanations. Additionally, while some may perceive cyber-stalking as "troubling behaviour" and "dating abuse", others may see it as a "monitory gadget" or a functional behaviour to help maintain a committed relationship. The internet does not exist in a vacuum, and the ways in which online behaviours and attitudes are extensions of offline social processes and relationships is also evidenced in the meaning of cyber-stalking. Arguably, this mismatch between these different age groups concerning the meaning of cyber-stalking, however trivial, suggests that, as Sheridan *et al.* (2016) noted, the meaning of cyber-stalking is largely socially constructed. While terms may appear to be objective, they are actually underpinned by value judgements that are rooted in particular cultural assumptions (Ribbens *et al.* 2011; Stambolis-Ruhstorfer and Saguy 2014).

Indeed, there is no objective viewpoint for the definition of an "immoral" act (Becker [1967] 1997; Reiner 2016). Cyber-stalking, as an action, could be interpreted in a negative or positive light depending on the perceived perpetrator–victim-gender structure. Also, while cyber-stalking may involve "behaviours that are ostensibly routine and harmless" (Sheridan *et al.* 2016, p.2), some people stalk to some extent even without any malicious intent, given that the boundary between socially acceptable courting and cyber-dating abuse is blurred (Choo *et al.* 2017). It could be that some people generally indulge in cyber-stalking at some point as a socially acceptable courting act. By implication, a variable minimum number of occurrences for the action to be considered as cyber-stalking may apply differently to each participant, given that its meaning is diffuse and it primarily occurs under the realm of "love" and romance (Marcum *et al.* 2017). In fact, it is the degree of prior intimacy between the victim and perpetrator that largely influences most people's perceptions of harm in cyber-stalking behaviours (Sheridan *et al.* 2016). Equally, cultural expectations and norms for romantic relationships offline extend and shape the meaning of cyber-stalking because people generally have diverse opinions as to what exactly constitutes cyber-stalking. The above studies highlight the need to understand gender differences in cyber-stalking. Relatedly, gender differences identified in all the above studies (on cyber-stalking, online harassment, cyber-bullying, cyber-fraud, and

© 2019 John Wiley & Sons Ltd

revenge porn) illuminate that the critical starting points for the analysis of gender and crimes are who is victimised, why and to what effect. Since psychosocial cybercrimes (e.g., cyber-stalking) could be more gendered than socioeconomic ones (e.g., cyber-fraud), the meaning of "cybercrime" is problematic, as previously argued. It is noteworthy that cyber-stalking (psychosocial cybercrime) has not been compared with socioeconomic crimes (e.g., digital piracy) to better understand their differences in the light of the TCF (and the feminist epistemology of crime).

4.6 A comparison of three digital crimes (case study) framed with mainstream criminology theory

A recent study (Donner 2016), which compares the forms of digital crimes (hacking, online harassment, and digital piracy), is framed with Gottfredson and Hirschi's (1990) General Theory of Crime. It contends that men were more likely to engage in online offending and that this gender gap was reasonably consistent across the board. In particular, this study found that men were more likely to engage in online harassment (psychosocial) and digital piracy (such as illegal downloads of items, i.e., socioeconomic), irrespective of self-control level, whereas "higher immersion into the cyber-environment resulted in men and women having similar rates of digital piracy" (i.e., a socioeconomic cybercrime) (Donner 2016, p.570), which suggests that perhaps socioeconomic cybercrime is less gendered than online harassment (psychosocial cybercrime) if viewed from the lens of the TCF.

Accordingly, this study's findings could have been a little more clearly and directly expressed had a more gender-sensitive framework been applied in place of a mainstream criminology lens. For instance, Donner (2016, p.571) acknowledged, "the findings revealed that, regardless of self-control level, men had higher rates [than women] of online offending almost across the board, which is inconsistent with the theory. Thus, it appears that gender may be more useful in explaining cybercrime than self-control, although self-control is more important for low self-control individuals, as it eliminated the gender difference in digital piracy". The author then recommends that "future researchers should consider utilising a bond-based measure of self-control, which would be more theoretically consistent with the revised version of the theory" (Donner 2016, p.572). These obscurities in reporting research findings nevertheless echo the suggestion that theories may be supportive or obstructive to the researchers' analytic capacity when they have more faith in the correctness of the theories than in the authenticity of their data (Greenwald *et al.* 1986). This therefore reinforces the notion that mainstream criminology theories may not be a "toolbox" for cyber or digital criminology inquiries, as in Rimer's (1997) term, as theology is for followers. By building on the extant literature, I argue here that who is victimised, why, and to what effect do not apply in the same way to socioeconomic cybercrimes as they do to psychosocial cybercrimes. Therefore, this article, framed with the TCF alongside the feminist epistemology of crime, advocates the centrality of gender as a theoretical starting point for the examination of the gender gap between psychosocial and socioeconomic cybercrime types.

Prompted by the above primary limitation, this article proposes that persisting with the umbrella term "cybercrime", the binary typologies, and some mainstream criminology theories, does not help us to understand how structured gender relations might retain their efficacy in online contexts because a person cannot be online without being offline. The lens of "cybercrime", as an umbrella term, and the binary typologies obscure the manifestation of gender cultures and nuances in multiple areas of social lives. These typologies and theories undermine a more critical examination of gender issues concerning a wide range of digital crimes. Framed with the TCF, this article has demonstrated that psychosocial cybercrimes could be more gendered than those which are socioeconomic. For example, as previously mentioned, Donner's (2016) paper demonstrated that digital piracy (socioeconomic cybercrime) was perceived similarly across sexes. On the flipside, as regards a range of psychosocial crimes such as cyber-bullying (e.g., Cunningham *et al.* 2015), revenge porn (e.g., Walker and Sleath 2017), cyber-stalking (e.g., Marcum *et al.* 2017), and online harassment (e.g., Barlett and Coyne 2014), numerous studies demonstrate that who is victimised, why, and to what effect are the critical entry points to the analysis of gender and crimes. It is plausible, therefore, to argue that the psychosocial category is more gendered than the socioeconomic category (e.g., digital piracy and cyber-fraud). Arguably, the TCF provides support

© 2019 John Wiley & Sons Ltd

for continuing to expand our analysis of gender issues in cyber criminology, as well as a more refined theoretical perspective for grouping a wide spectrum of cybercrime types above. Thus, as Eagly (2016) and Wood and Eagly (2010) illuminate, rather than discounting, the existence of sex-related differences, such differences and similarities are reflections of cultural nuances and norms of social interaction.

5. Conclusion

While this article has underscored the utilitarian value of the TCF, it aligns it with feminist criminology perspectives. It accentuates that it is of the utmost importance for the umbrella term "cybercrime" and most mainstream criminology theories to be revisited, redefined, and reconstructed because they have huge consequences. They have, for example, obscured the centrality of gender as a theoretical starting point for examining a multitude of digital crimes in academia. Such theoretical and methodological oversights in research, in turn, have real-life repercussions. A likely consequence of these omissions is that many corporations and government agencies may not fully recognise the importance of gender and crime connections in their responses to many forms of digital crime.

I recommend that researchers on "cyber criminology" or "digital criminology" should unconditionally take on board the feminist criminology agenda, given that many digital crimes may not possess the same features as the traditional ones from which they have emerged. Indeed, a greater computer expertise on the part of women (and girls) may realign the prevailing men/women unequal power relation associated with perpetrator/victim traditional crimes. Mere proficiency in ICT and immersion in cyber-environments may reshape patterns of offending and victimisation for crimes that depend primarily on ICT skills.

Fundamentally, this paper is a theoretical endeavour that advocates the centrality of gender as a conceptual starting point for investigations in cyber criminology. Building on previous works that have critiqued mainstream criminology (e.g., Cook 2016; hooks [1984] 2000; Sharp 2015), this article argues that more has to be done to wake criminology from its "androcentric slumber". Accordingly, this paper has attempted to stimulate contemporary scholarly endeavours to be more alert or sensitive to gender issues. It has attempted to stimulate scholars to situate the feminist epistemology of crime at the core of criminology enquiries, because generations after generations of scholars who are unaware of feminist criminology as students concomitantly teach their students mainstream theories at the expense of feminist approaches (Sharp 2015), as discussed above. Consequently, only the marginal voices whose endeavours fit squarely with the aims and scopes of marginal publication venues (often with "low or average impact factors") tend to challenge the orthodoxy of mainstream criminology.

As long as the term "cybercrime", the binary typologies, and most mainstream criminology theories are taken as a given in cyber criminology research (and influence researchers the way theology does believers), windows of opportunities necessary to advance our understanding of gender and a range of digital crimes will continue to be limited. Additionally, this article has not only demonstrated that structured gender relations retain their efficacy in online contexts, but it has also illustrated what gender is and that women and men do interact with other categories (e.g., age and sexuality) to influence the experiences of victims of digital crimes. Thus, the article has not only benefited from the lens of TCF but also from an additional lens. Simply put, by employing the lens of digital intersectionality, it has considered other categories of social (dis)advantages to answer the question: do structured gender relations retain their efficacy in online contexts?

While this paper has benefited from the advancement of the TCF, the TCF itself is, however, not immune to limitations. Mainly, the TCF is somewhat simplistic. Given that the apparent boundaries between TCF's categories are blurred, they could be seen as a loose grouping of cybercrime types. A complex web of hybrid forms of crimes on the internet exposes the TCF's weakness. For example, cyberbullying could eventually lead to cyber-extortion, or hacktivists exposing stolen personal data from police officers, as a political protest could have psychosocial and geopolitical consequences at the same time (as shown in Table 1). Although the TCF has flaws, it has useful contributions in spite of them. It has attempted to move gender analysis of digital crimes "from margin to centre". We will accomplish more, and quicker, if we consider this current endeavour as an avenue to situate the

© 2019 John Wiley & Sons Ltd

feminist perspectives at the core of cyber criminology enquiries. Future research is needed to strengthen the synergy between the TCF and the feminist epistemology of crime.

Acknowledgments

I thank Jane McCarthy and Sally Mann for their useful comments on parts of my preliminary draft.

Notes

1. While there are many examinations of girls/women and crime that are not feminist, there are men who are feminist criminologists, and there are many women in criminology who are not feminist (Sharp 2015).

2. However, some mainstream theorists have acknowledged the importance of incorporating feminist approaches into criminology as a field of study (Broidy and Agnew 1997).

3. Social (dis)advantage – inequality in the central and value things people are able to be or do (Dean and Platt 2016).

4. However, the legal and cultural contexts vary across nations (Jones 2018).

5. These six online crimes outlined resonate with the original formulation of the TCF.

6. It is noteworthy that the turmoil associated with adolescence may vary across different measures and social contexts (Schneider and Csikszentmihalyi 2017).

7. Listed in the prevalence of cybercrime perpetrators, Nigeria, the United Kingdom, and the United States (in ascending order of significance) are at the top of the FBI's (2010) "league table". However, a critical examination has pointed out that the statistics the FBI relied upon to inform the current state of cybercrime perpetrators across nations, even when they represent the underlying reality, are socially and selectively constructed – the FBI's statistics, therefore, cannot (or should not) directly speak for themselves (Ibrahim 2016, pp.50–52).

8. Even men's adulterous undertakings are culturally seen as an additional layer of prestige (Smith 2017).

9. In Nigeria, for example, "most cybercriminals involved in stealing panties for money rituals are exclusively involved in stealing women's panties, sometimes at gun/knife points" (Lazarus 2019, p.10).

10. Walker and Sleath (2017) review of 82 published studies from the US (n=48), Australia (n=13), the UK (n=5), Spain (n=5), Italy (n=2), Canada (n=3), Sweden (n=1), Thailand (n=1), Germany (n=1), Switzerland (n=1), Belgium (n=1), and others from unidentified countries.

References

Adebanjo, A.T., 2015. Culture, morality and the law: Nigeria's anti-gay law in perspective. *International journal of discrimination and the law*, 15 (4), 256–270.

Agboola, C. and Rabe, M., 2018. Intersectionality and crime: reflections from female ex-inmates in South Africa. *Acta criminologica: Southern African journal of criminology*, 31 (1), 1–18.

Al Izki, F. and Weir, G.R., 2015. Gender impact on information security in the Arab world. *In*: *International conference on global security, safety, and sustainability* (pp. 200–207). Cham: Springer.

Aransiola, J.O. and Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, behavior, and social networking*, 14 (12), 759–763.

Aricak, M.T., 2009. Psychiatric symptomatology as a predictor of cyberbullying among university students. *Eurasian journal of education research*, 34, 167–184.

Bae, S.M., 2017. The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and youth services review*, 78, 74–80.

Ball, M., Lenning, E. and Buist, C.L., 2018. *Queer criminology*. London: Routledge.

Barlett, C. and Coyne, S.M., 2014. A meta-analysis of sex differences in cyber-bullying behavior: the moderating role of age. *Aggressive behavior*, 40 (5), 474–488.

Baym, N.K. and Boyd, D., 2012. Socially mediated publicness: an introduction. *Journal of broadcasting & electronic media*, 56 (3), 320–329.

Becker, H., [1967]1997. *Outsiders: studies in sociology of deviance*. New York: Simon and Schuster Ltd.

© 2019 John Wiley & Sons Ltd

Beckman, L., Hagquist, C. and Hellström, L., 2013. Discrepant gender patterns for cyberbullying and traditional bullying – an analysis of Swedish adolescent data. *Computers in human behavior*, 29 (5), 1896–1903.

Berger, K.S., 2007. Update on bullying at school: science forgotten? *Developmental review*, 27 (1), 90–126.

Bidgoli, M. and Grossklags, J., 2016. End user cybercrime reporting: what we know and what we can do to improve it. *In*: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada, (pp. 1–6).

Boakye, K.E., 2013. Correlates and predictors of juvenile delinquency in Ghana. *International journal of comparative and applied criminal justice*, 37 (4), 257–278.

Boulton, M., Lloyd, J., Down, J. and Marx, H., 2012. Predicting undergraduates' self-reported engagement in traditional and cyberbullying from attitudes. *Cyberpsychology, behavior, and social networking*, 15 (3), 141–147.

Braithwaite, A., 2014. "Seriously, get out": feminists on the forums and the war (craft) on women. *New media & society*, 16 (5), 703–718.

Braithwaite, J., 1989. *Crime, shame, and reintegration*. Cambridge, UK: Cambridge University Press.

Broidy, L. and Agnew, R., 1997. Gender and crime: a general strain theory perspective. *Journal of research in crime and delinquency*, 34 (3), 275–306.

Buist, C., and Lenning, E., 2015. *Queer criminology*. New York: Routledge.

Burgess-Proctor, A., 2006. Intersections of race, class, gender, and crime: future directions for feminist criminology. *Feminist criminology*, 1(1), 27–47.

Button, M. and Cross, C., 2017. *Cyber frauds, scams and their victims*. London: Routledge.

Cartwright, B.E., 2016. Cyberbullying and cyber law. *In*: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada, (pp. 1–7).

Chen, P., Kokbayashi, E., Vazsonyi, A. and Sharp, S., 2010. A culturally nuanced test of Gottfredson and Hirschi's "General Theory": dimensionality and generalizability in Japan and the United States. *International criminal justice review*, 20 (2), 112–131.

Choo, K.K.R., Eterovic-Soric, B., Ashman, H. and Mubarak, S., 2017. Stalking the stalkers – detecting and deterring stalking behaviours using technology: a review. *Computers & security*, 70, 278–289.

Citron, D.K., 2014. *Hate crimes in cyberspace*. London: Harvard University Press.

Connell, R.W. and Messerschmidt, J., 2005. Hegemonic masculinity: rethinking the concept. *Gender and society*, 19, 829–859.

Cook, K.J., 2016. Has criminology awakened from its "androcentric slumber"? *Feminist criminology*, 11 (4), 334–353.

Cunningham, C.E., Chen, Y., Vaillancourt, T., Rimas, H., Deal, K., Cunningham, L. J. and Ratcliffe, J., 2015. Modeling the anti-cyberbullying preferences of university students: adaptive choice-based conjoint analysis. *Aggressive behavior*, 41 (1), 369–385.

Daly, K. and Chesney-Lind, M., 1988. Feminism and criminology. *Justice quarterly*, 5, 497–538.

Dean, H. and Platt, L., 2016. *Social advantage and disadvantage*. Oxford: Oxford University Press.

Donner, C.M., 2016. The gender gap and cybercrime: an examination of college students' online offending. *Victims & offenders*, 11 (4), 556–577.

Donner, C.M., Jennings, W.G. and Banfield, J., 2015. The general nature of online and off-line offending among college students. *Social science computer review*, 33 (6), 663–679.

Drouin, M., Vogel, K.N., Surbey, A. and Stills, J.R., 2013. Let's talk about sexting, baby: computer-mediated sexual behaviors among young adults. *Computers in human behavior*, 29 (5), A25–A30.

Eagly, A.H., 2016. IV. Has the psychology of women stopped playing handmaiden to social values? *Feminism & psychology*, 26 (3), 282–291.

Eckert, S., 2018. Fighting for recognition: online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States. *New media & society*, 20 (4), 1282–1302.

Eklund, L., 2011. Doing gender in cyberspace: the performance of gender by female World of Warcraft players. *Convergence*, 17 (3), 323–342.

Englander, E., Donnerstein, E., Kowalski, R., Lin, C.A. and Parti, K., 2017. Defining cyberbullying. *Pediatrics*, 140, S148–S151.

Efthymiou, A. and Stavrakakis, H., 2018. Rap in Greece: Gendered configurations of power in-between the rhymes. *Journal of Greek Media & Culture*, 4 (2), 205–222.

Everbach, T., 2018. "'I Realized It Was About Them . . . Not Me': Women Sports Journalists and Harassment." In Mediating Misogyny: Gender, Technology, and Harassment edited by Jacqueline Ryan Vickery and Tracy Everbach, 131–150. Cham, Switzerland: Palgrave Macmillan.

Faucher, C., Jackson, M. and Cassidy, W., 2014. Cyberbullying among university students: gendered experiences, impacts, and perspectives. *Education research international*. Retrieved from: https://www.hindawi.com/journals/edri/2014/698545/abs/ [11 November 2017].

FBI, 2010. Internet crime complaint centre. Retrieved from: https://pdf.ic3.gov/2010_IC3Report.pdf [9 September 2017].

FBI, 2016. Internet crime schemes. Available at: https://www.ic3.gov/crimeschemes.aspx#item-13 [28 January 2018].

Finn, J., 2004. A survey of online harassment at a university campus. *Journal of interpersonal violence*, 19 (4), 468–483.

© 2019 John Wiley & Sons Ltd

Flavin, J., 2001. Feminism for the mainstream criminologist: an invitation. *Journal of criminal justice*, 29 (4), 271–285.

Fogiel-Bijaoui, S., 2016. The cosmopolitan future: a feminist approach. *Laws*, 5 (3), 34.

Freud, S., [1927]1991. *Civilization, society and religions: group psychology and the analysis of the ego, future of an illusion and civilization and its discontents*. New York: Penguin Books Ltd.

Garnett-Bower, C.I., 2017. *Juveniles and cyberstalking: public perception of offender dangerousness*. Thesis (PhD). Alliant International University.

Geis, G., 2000. On the absence of self-control as the basis for a general theory of crime: a critique. *Theoretical criminology*, 4 (1), 35–53.

Gordon, S. and Ford, R., 2006. On the definition and classification of cybercrime. *Journal in computer virology*, 2 (1), 13–20.

Gottfredson, M. and Hirschi, T., 1990. *A general theory of crime*. Stanford, CA: Stanford University Press.

Greenwald, A., Pratkanis, A, Leippe, M. and Baumgardner, M., 1986. Under what conditions does theory obstruct research progress? *Psychological review*, 93, 216–229.

Hazen, E., Schlozman, S. and Beresin, E., 2008. Adolescent psychological. *Pediatrics in review*, 29 (5), 161.

Helsper, E.J. and Whitty, M.T., 2010. Netiquette within married couples: agreement about acceptable online behavior and surveillance between partners. *Computers in human behavior*, 26 (5), 916–926.

Hill, J.B. and Marion, N.E., 2016. Presidential rhetoric and cybercrime: tangible and symbolic policy statements. *Criminology, crim. justice, law & society*, 17 (2), 1–17.

Holt, T.J., Bossler, A.M. and May, D.C., 2012. Low self-control, deviant peer associations, and juvenile cyberdeviance. *American journal of criminal justice*, 37 (3), 1–18.

Hooks, B., [1984]2000. *Feminist theory: from margin to center*. New York: Pluto Press.

Hutchings, A. and Chua, Y., 2017. Gendering cybercrime. *In*: Holt, T.J. ed. *Cybercrime through an interdisciplinary lens* (pp. 167–188). New York: Routledge.

Ibrahim, S., 2015. A binary model of broken home: parental death-divorce hypothesis of male juvenile delinquency in Nigeria and Ghana *In*: Maxwell, S.R. and Blair, S.L. eds. *Contemporary perspectives in family research*, Vol. 9 (pp. 311–340). New York: Emerald Group Publishing Limited.

Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. *International journal of law, crime and justice*, 47, 44–57.

Ibrahim, S., 2017. Causes of socioeconomic cybercrime in Nigeria. *In*: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada, (pp. 1–9).

Ibrahim, S. and Komulainen, S., 2016. Physical punishment in Ghana and Finland: criminological, sociocultural, human rights and child protection implications. *International journal of human rights and constitutional studies*, 4 (1), 54–74.

Jaishankar, K., 2007. Cyber criminology: evolving a novel discipline with a new journal. *International journal of cyber criminology*, 1(1), 1–6.

Jaishankar, K., 2011. *Expanding cyber criminology with an avant-garde anthology* (Introduction). Boca Raton, Florida: CRC Press, Taylor and Francis Group.

James, A., 2010. School bullying. Research briefing. Downloaded from: www.nspcc.org.uk/inform, 26, 2012.

Jane, E.A., 2016a. Online misogyny and feminist digilantism. *Continuum*, 30 (3), 284–297.

Jane, E.A., 2016b. *Misogyny online: a short (and brutish) history*. London: Sage.

Jegede, A.E., Elegbeleye, A.O., Olowookere, E.I. and Olorunyomi, B.R., 2016. Gendered alternative to cyber fraud participation: an assessment of technological driven crime in Lagos State, Nigeria. *Gender and behaviour*, 14 (3), 7672–7692.

Jones, M.L., 2018. *Ctrl+ Z: the right to be forgotten*. New York: NYU Press.

Kirillova, E.A., Kurbanov, R.A., Svechnikova, N.V., Zul'fugarzade, T.E.D. and Zenin, S.S., 2017. Problems of fighting crimes on the internet. *Journal of advanced research in law and economics*, 8 (3), 849–856.

Klenowski, P.M., Copes, H. and Mullins, C. W., 2011. Gender, identity, and accounts: how white collar offenders do gender when making sense of their crimes. *Justice quarterly*, 28 (1), 46–69.

Kraft, E. and Wang, J., 2010. An exploratory study of the cyberbullying and cyberstalking experiences and factors related to victimization of students at a public liberal arts college. *International journal of technoethics*, 1 (4), 74–91.

Larson, R. and Ham, M., 1993. Stress and "stormy and stress" in early adolescence: the relationship of negative events with dyphoric affect. *Developmental psychology*, 29 (1),130–140.

Lavee, E. and Benjamin, O., 2017. Between social rights and human rights: Israeli mothers' right to be protected from poverty and prostitution. *Journal of comparative family studies*, 48 (3), 315–326.

Lazarus, S., 2018. Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo boys) and hip hop artists. *Criminology, criminal justice, law & society*, 19 (2), 63–81.

Lazarus, S., 2019. Where is the money? The intersectionality of the spirit world and the acquisition of wealth. *Religions*, 10 (3), 146, 1–20.

Lazarus, S., Rush, M., Dibiana, E.T. and Monks, C.P., 2017. Gendered penalties of divorce on remarriage in Nigeria: a qualitative study. *Journal of comparative family studies*, 48 (3), 351–366.

© 2019 John Wiley & Sons Ltd

Lazarus, S. and Uzoma Okolorie, G., 2019. The bifurcation of Nigerian cybercriminals: narratives of the Economic and Financial Crimes Commission (EFCC) agents. Telematics and Informatics, p.1–14, https://doi.org/10.1016/j.tele.2019.04.009.

Lindsay, M. and Krysik, J., 2012. Online harassment among college students: a replication incorporating new internet trends. *Information, communication & society*, 15 (5), 703–719.

Lynch, M.J., 2016. Acknowledging female victims of green crimes: environmental exposure of women to industrial pollutants. *Feminist criminology*, 13 (4), 404–427.

Maldonado-Molina, M.M., Piquero, A.R., Jennings, W.G., Bird, H. and Canino, G., 2009. Trajectories of delinquency among Puerto Rican children and adolescents at two sites. *Journal of research in crime and delinquency*, 46, 144–181.

Marcum, C.D., Higgins, G.E. and Nicholson, J., 2017. I'm watching you: cyberstalking behaviors of university students in romantic relationships. *American journal of criminal justice*, 42 (2), 373–388.

Marcum, C.D., Higgins, G.E., Freiburger, T.L. and Ricketts, M.L., 2012. Battle of the sexes: an examination of male and female cyber bullying. *International journal of cyber criminology*, 6 (1), 904–911.

McGerty, L.J., 2000. "Nobody lives only in cyberspace": gendered subjectivities and domestic use of the internet. *CyberPsychology & behavior*, 3 (5), 895–899.

McGuire, M. and Dowling, S., 2013. Cybercrime: a review of the evidence. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf [28 September 2017].

Morahan-Martin, J., 2000a. Women and the internet: promise and perils. *CyberPsychology & behavior*, 3 (5) 683–691.

Morahan-Martin, J., 2000b. The gender gap in internet use: why men use the internet more than women. *CyberPsychology & behavior*, 1 (1), 3–10.

Mumporeze, N. and Prieler, M., 2017. Gender digital divide in Rwanda: a qualitative analysis of socioeconomic factors. *Telematics and informatics*, 34 (7), 1285–1293.

Naegler, L. and Salman, S., 2016. Cultural criminology and gender consciousness: moving feminist theory from margin to center. *Feminist criminology*, 11 (4), 354–374.

Näsi, M., Oksanen, A., Keipi, T. and Räsänen, P., 2015. Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian studies in criminology and crime prevention*, 16 (2), 203–210.

National Crime Agency, 2017. Cybercrime. Available at: http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime [7 July 2017].

Newburn, T., 2016. Social disadvantage: crime and punishment. *In*: Dean, H. and Platt, L. eds. *Social advantage and disadvantage* (pp. 322–340). Oxford: Oxford University Press.

Norton by Symantec, 2015. What is cybercrime? Retrieved from: http://nz.norton.com/cybercrime-definition [26 July 2016].

Oakley, A., 2018. *From here to maternity (reissue): becoming a mother*. Croydon: Policy Press.

Ojanen, T.T., Boonmongkon, P., Samakkeekarom, R., Samoh, N., Cholratana, M. and Guadamuz, T.E., 2015. Connections between online harassment and offline violence among youth in central Thailand. *Child abuse & neglect*, 44, 159–169.

Potter, H., 2015. *Intersectionality and criminology: disrupting and revolutionizing studies of crime*. New York, NY: Routledge.

Powell, A., Stratton, G. and Cameron, R., 2018. *Digital criminology: crime and justice in digital society*. London: Routledge.

Priebe, G. and Svedin, C.G., 2012. Online or off-line victimisation and psychological well-being: a comparison of sexual-minority and heterosexual youth. *European child & adolescent psychiatry*, 21 (10), 569–582.

Purcell, R., Pathe, M. and Mullen, P.E., 2001. A study of women who stalk. *American journal of psychiatry*, 158 (12), 2056–2060.

Purcell, R., Pathe, M. and Mullen, P., 2009. Gender differences in stalking behavior among juveniles. *Journal of forensic psychiatry and psychology*, 21 (4), 555–568.

Purcell, R., Pathe, M. and Mullen, P.E., 2010. Gender differences in stalking behaviour among juveniles. *Journal of forensic psychiatry & psychology*, 21 (4), 555–e568. Available at: http://doi.org/10.1080/14789940903572035.

Reiner, R., 2016. *Crime, the mystery of the common-sense concept*. New York: John Wiley & Sons.

Ribbens McCarthy, J. and Edwards, R., 2011. *Key concepts in family studies*. London: Sage Publications.

Richardson, S.V.A. and Gilmour, N., 2015. Cyber crime and national security: a New Zealand perspective. *European review of organised crime*, 1 (1), 51–70.

Rimer, B., 1997. Perspectives on intrapersonal theories of health behavior. *In*: Glanz, K., Lewis, F. and Rimer, B. eds. *Health behaviour and health education: theory, research and practice* (pp. 139–147). Jossey-Bass, San Francisco, CA.

Rokven, J.J., Weijters, G., Beerthuizen, M. G. van der Laan, A.M., 2018. Juvenile delinquency in the virtual world: similarities and differences between cyber-enabled, cyber-dependent and offline delinquents in the Netherlands. *International journal of cyber criminology*, 12 (1), 27–46.

Rosch, E., 1978. Principles of categorization. *In*: Rosch, E. and

© 2019 John Wiley & Sons Ltd

Lloyd, B.B. eds. *Cognition and categorizatio*n (pp. 27–48). Hillsdale, NJ: Lawrence Erlbaum Associates.

Rosenbach E. and Belk, R., 2012. U.S. cybersecurity: the current threat and future challenges. *In*: Burns, N. and Price, J. eds. *Securing cyberspace – a new domain for national security*. Washington, DC: The Aspen Institute.

Rush, M. and Lazarus, S., 2018. "Troubling" chastisement: a comparative historical analysis of child punishment in Ghana and Ireland. *Sociological research online*, 23 (1), 177–196.

Sabillon, R., Cavaller, V., Cano, J. and Serra-Ruiz, J., 2016. Cybercriminals, cyberattacks and cybercrime. *In*: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada, (pp. 1–9).

Sabon, L.C., 2016. Force, fraud, and coercion – what do they mean? A study of victimization experiences in a new destination Latino Sex Trafficking Network. *Feminist criminology*, 13 (5), 456–476.

Schenk, A.M. and Fremouw, W.J., 2012. Prevalence, psychological impact, and coping of cyberbully victims among college students. *Journal of school violence*, 11, 21–37.

Schiebinger, L., 2000. Has feminism changed science? *Signs: journal of women in culture and society*, 25 (4), 1171–1175.

Schneider, B. and Csikszentmihalyi, M., 2017. Conditions for optimal development in adolescence: an experiential approach. *In*: *Conditions for optimal development in adolescence* (pp. 122–124). New York: Psychology Press.

Schoepfer, A., Baglivio, M. and Schwartz, J., 2017. Juvenile hybrid white-collar delinquency: an empirical examination of various frauds. *Criminology, criminal justice law and society*, 18 (2), 21–38.

Sharp, F.S., 2015. Feminist criminology and gender studies. *International encyclopedia of the social & behavioral sciences*, 2 (8), 912–917.

Sheridan, L., Scott, A. J. and Nixon, K., 2016. Police officer perceptions of harassment in England and Scotland. *Legal and criminological psychology*, 21 (1), 1–14.

Sherman, R.C., End, C., Kraan, E., Cole, A., Campbell, J., Birchmeier, Z. and Klausner, J., 2000. The internet gender gap among college students: forgotten but not gone? *Cyberpsychology, Behavior, and Social Networking*, 3 (5), 885–894.

Smith, D.J., 2017. *To be a man is not a one-day job: masculinity, money, and intimacy in Nigeria*. Chicago: University of Chicago Press.

Smith, P.K., 2012. Cyberbullying and cyber aggression. *In*: Jimerson, S.R., Nickerson, A.B., Mayer, M.J. and Furlong, M.J. eds. *Handbook of school violence and school safety: international research and practice*, 2nd ed. (pp. 93–103). New York: Routledge.

Smoker, M. and March, E., 2017. Predicting perpetration of intimate partner cyberstalking: gender and the dark tetrad. *Computers in human behavior*, 72, 390–396.

Stambolis-Ruhstorfer, M. and Saguy, A.C., 2014. How to describe it? Why the term coming out means different things in the United States and France. *Sociological forum*, 29 (4), 808–829.

Tan, H.K. and David, Y., 2017. Preying on lonely hearts: a systematic deconstruction of an internet romance scammer's online lover persona. *Journal of modern languages*, 23 (1), 28–40.

Tynes, B.M., Schuschke, J. and Noble, S.U., 2016. Digital intersectionality theory and the black matter movement. *In*: Noble, S.U. and Tynes, B.M., eds. *The intersectional internet: race, sex, class, and culture online*. Berlin: Peter Lang International Academic Publishers.

Vasilescu, B., Capiluppi, A. and Serebrenik, A., 2012. Gender, representation and online participation: a quantitative study of stackoverflow. *In*: IEEE *International Conference on Social Informatics* (pp. 332–338). IEEE.

Walker, K. and Sleath, E., 2017. A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and violent behavior*, 36, 9–24.

Watts, L.K., Wagner, J., Velasquez, B. and Behrens, P.I., 2017. Cyberbullying in higher education: a literature review. *Computers in human behavior*, 69, 268–274.

Weitzer, R. and Kubrin, C.E., 2009. Misogyny in rap music: a content analysis of prevalence and meanings. *Men and masculinities*, 12 (1), 3–29.

West C. and Zimmerman, D.H., 1987. Doing gender. *In*: Fenstermaker, S. and West, C. eds. *Doing gender, doing difference* (pp. 3–24). New York: Routledge.

Whitty, M.T. and Buchanan, T., 2012. The online romance scam: a serious cybercrime. *CyberPsychology, behavior, and social networking*, 15 (3),181–183.

Whitty, M.T. and Buchanan, T., 2016. The online dating romance scam: the psychological impact on victims – both financial and non-financial. *Criminology & criminal justice*, 16 (2), 176–194.

Wood, W. and Eagly, A.H., 2010. Gender. *In*: Fiske, S.T., Gilbert, D.T. and Lindzey, G. eds. *Handbook of social psychology* (Vol. 1) 5th ed. (pp. 629–667). Hoboken, NJ: Wiley.

Yar, M., 2017. Online crime. *In*: Pontell, H. ed. *Oxford research encyclopedia of criminology: criminology & criminal justice*. Oxford: Oxford University Press.

Zietz, D., 1981. *Women who embezzle or defraud: a study of convicted felons*. New York: Praeger.

Zupan, L.L., 1986. Gender-related differences in correctional officers' perceptions and attitudes. *Journal of criminal justice*, 14 (4), 349–361.

© 2019 John Wiley & Sons Ltd

Telematics and Informatics 40 (2019) 14–26

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents

Suleman Lazarus[a,*], Geoffrey U. Okolorie[b,c]

[a] University of Greenwich, United Kingdom
[b] University of Derby, United Kingdom
[c] Economic and Financial Crimes Commission (EFCC), Nigeria

ARTICLE INFO

Keywords:
Nigerian cyber-fraudsters
Narratives of law enforcement officers
Bifurcation of Yahoo Boys
Masculinity and symbolic interaction
Cybercrime and cultural relativism
Spiritual dimension of cybercrime

ABSTRACT

While this article sets out to advance our knowledge about the characteristics of Nigerian cybercriminals (Yahoo-Boys), it is also the first study to explore the narratives of the Economic and Financial Crimes Commission (EFCC) officers concerning them. It appraises symbolic interactionist insights to consider the ways in which contextual factors and worldview may help to illuminate officers' narratives of cybercriminals and the interpretations and implications of such accounts. Semi-structured interviews of forty frontline EFCC officers formed the empirical basis of this study and were subjected to a directed approach of qualitative content analysis. While prior studies, for example, indicated that only a group of cybercriminals deploy spiritual and magical powers to defraud victims (i.e. modus operandi), our data analysis extended this classification into more refined levels involving multiple features. In particular, analysis bifurcates cybercriminals and their operations based on three factors: educational-attainment, modus-operandi, and networks-collaborators. Results also suggest that these cybercriminals and their operations are embedded in "masculinity-and-material-wealth". These contributions thus have implications for a range of generally accepted viewpoints about these cybercriminals previously taken-for-granted. Since these criminals have victims all over the world, insights from our study may help various local and international agencies [a] to understand the actions/features of these two groups of cybercriminals better and develop more effective response strategies. [b] to appreciate the vulnerabilities of their victims better and develop more adequate support schemes. We also consider the limitations of social control agents' narratives on criminals.

1. Introduction

"*I went to Nigeria to meet the man who scammed me*"

In Nigeria, over 77% of youths live on less than USD2 per day (African Development Bank, 2018), and online and offline lives are inextricably intertwined (Lazarus, 2019a, b; Powell et al., 2018). Even though the link between offending and poverty is far from straightforward (Newburn, 2016), unemployment and poverty have strong connections with online crimes "within a given nation" (Kigerl, 2012, p. 483). What is notable is that the Nigerian youths have been disproportionately implicated in defrauding victims all over the world (Akanle et al., 2016). Internet crimes are global issues (Kirillova et al., 2017; Wall, 2007; Yar, 2017), and millions of people with email accounts have undoubtedly encountered Nigerian scam emails (Rich, 2017). Consequently, recent years have

* Corresponding author.
E-mail addresses: suleman.lazarus@gmail.com (S. Lazarus), okolorieu@yahoo.co.uk, gokolorie@efccnigeria.org (G.U. Okolorie).

https://doi.org/10.1016/j.tele.2019.04.009
Received 18 September 2018; Received in revised form 23 January 2019; Accepted 23 April 2019
Available online 24 April 2019
0736-5853/ © 2019 Elsevier Ltd. All rights reserved.

witnessed an upsurge of research on victims of cyber-fraud that supposedly originates from Nigeria (e.g. Cross et al., 2018; Owen et al., 2017; Sorell and Whitty, 2019). We still, however, know very little about Nigerian cyber-fraudsters (Lazarus, 2018). Remarkably, no study has attempted to explore the narratives of officers who have close interactions with these cybercriminals, even though frontline law enforcement officers who routinely investigate, arrest, interview, interrogate and prosecute these cyber-fraudsters have insiders' insights. The narratives of these frontline law enforcement officers, therefore, merit examination. This study asks: "what are the narratives of frontline law enforcement officers about cyber-fraudsters and their activities in Nigeria?".

This contextual inquiry concerns the Nigerian cybercriminals, the narratives of law enforcement agents on the ground about these cybercriminals, and the implications of these narratives. A primary objective of this study is to shed light on the characteristics of the Nigerian cyber-fraudsters. Doing so is prompted by a central motive: to enlighten government agencies around the world about these cybercriminals so that they are in a better position to: [a] understand the actions/features of these cybercriminals better and develop more effective response strategies; and [b] appreciate the vulnerabilities of their victims better and develop more adequate support schemes. The study examines life on the ground in Nigeria and Nigerian law enforcement officers' own thoughts about cyber-fraud and cybercriminals. Since situations must be understood from the inside, this article sets out to explore the narratives of people (social actors) regarding their fellow men and women, which are the most meaningful within their particular cultural dynamics. Since cyber-frauds are social products, they must also be read, in Hayward and Young's (2004, p. 259) words, "in terms of the meanings they carry." This article assesses the connections between the indigenous worldview and cyber-fraud activities, looking for, in Swidler's (1990) terminology, the empirical traces of "culture in action." In particular, it harnesses law enforcement officers' narratives on cybercriminals and their activities to shed light on how indigenous worldviews may be connected with offending in the virtual world. Henceforth, the article is presented in five sections [i.e. section 2 to 6]: Firstly, the literature review (section 2) attempts to position the research topic within the existing literature by providing an overview of what we currently know, which helps to shed light on the phenomenon we are investigating. The literature review is followed by a theoretical background (i.e. section 3), which provides a lens from which to analyse, interpret and discuss data. The article then presents the remaining three sections in the following order: method (section 4), findings/discussion (section 5) and conclusion (section 6).

2. Literature review

2.1. Indigenous worldviews on wealth acquisition

Contexts are the resources for understanding "the ways in which local worldviews on wealth acquisition give rise to contemporary manifestations of spirituality in cyberspace" (Lazarus, 2019a, p.1). Indigenous spiritual worldviews are central to the discussion of wealth acquisition and the meaning of such wealth within the particular cultural dynamics from which they have emerged (Akanle and Adejare, 2018; Ellis, 2016). Many Nigerians "feed on the red blood corpuscles of the primal world and spiritual shrines" to generate material wealth (Kalu, 2002, p. 674; see also Ekeh, 1975). In this respect, "the intersectionality of the spiritual world and the acquisition of wealth" discussed in Lazarus's (2019a) recent work is revealing. While some Nigerians tap into religious resources for wealth accumulation, it is a misconception to group all such people into just one group (Lazarus, 2019a). Indeed, there is a distinction between benevolent and malevolent intentionality and, consequently, tapping into religious resources for wealth accumulation could be "licit or illicit" (Lazarus, 2019a, p.12). Either way, spirituality is a "critical factor in the activities of the criminals involved in organized and non-organized crimes" (Melvin and Ayotunde, 2010, p. 364). Life in the virtual world embodies cultural nuances in society (Jones, 2018; Powell et al., 2018). Thus, Lazarus (2019a), by specifically exploring the occult economy in a variety of different manifestations, concluded that the physical world concurrently extends into the virtual world as far as the aquisition of wealth is concerned. The occult economy can be defined as the deployment, real or imagined, of spiritual/magical means for material ends (Comaroff and Comaroff, 1999). Given that earthly riches are believed by some Nigerians to have a spiritual etiology (Ekeh, 1975; Ellis, 2016; Kalu, 2002), this worldview has consequences for many Nigerian institutions.

Traditional shrines, churches, and many religious institutions generally serve as "lubricants of commercial relationships' between spiritualist and ordinary Nigerians" (Ellis, 2016, p. 195). In this way, the spiritual world maintains its efficacy as the true source of wealth and its cultural potency is continuously legitimized, produced, and reproduced through interactional processes between ordinary citizens and the spiritualists (Lazarus, 2019a). Through these processes, a client–patron relationship between the gatekeepers of the shrines and sacred sites and ordinary citizens is negotiated and nurtured (Ekeh, 1975; Ellis, 2016). In turn, the cultural and symbolic "handshaking" between clients and patrons not only helps to harness this type of relationship, but it also blurs the boundary between the meaning of "bribe" and that of "*dash*" (Lazarus, 2019a). "*Dash*" is a local term for a gift in a Nigerian context. The exchanges of "*dashes*" between the representatives of many institutions, such as banks and ordinary Nigerians, including cybercriminals, are commonplace (e.g. Aransiola and Asindemade, 2011; Ibrahim, 2017). The underlying factor is that, while bribery and corruption are symptoms and outcomes of institutional deficiency (Dasgupta and Ugur, 2011; Ellis, 2016), expertise in bribery has been culturally deemed necessary, and sufficient, for holders of public posts to be successful in Nigeria (Ellis, 2016). These money-oriented social/cultural processes in Nigerian society extend to cyberspace and, consequently, have implications for this article's positioning.

2.2. Cybercrime and cultural relativism

Many scholars (e.g. Bae, 2017; Donner et al., 2015; Hutchings and Chua, 2017; Ibrahim, 2016; Lazarus, 2019b; Selwyn, 2008; Yar, 2017) have observed that the term "cybercrime" is an umbrella term for a wide spectrum of crimes, such as revenge pornography, cyber-stalking,

cyber-bullying, cyber-espionage, and cyber-fraud. For Wall (2007, p. 185), for example "cybercrimes are the product of networked computers, [and] must be defined in terms of the informational, networked, and globalised transformation of deviant or criminal behaviour by networked technologies". However, 'a computer may be materially the same, but placed in different cultures, a computer holds different meanings and generates different problems shaped by cultural factors in which the computer sits' (Jones, 2018 p. 18). To search for empirical clues of "culture in action" (Swidler, 1990), therefore, this study mobilizes marginal literature about the cultural dynamics of Nigerian cyber-fraudsters, as Cross's (2018) comprehensive literature review suggested. The above author elaborated that the narratives of current cyber-fraud research are only reflective of the mainstream perspectives at the expense of the marginalised voices. In other words, the voices of scholars from the global South especially Nigeria, are ignored, and by implication, the narratives of scholars from the global North exclusively inform the global cyber-fraud discourse. A better understanding of this phenomenon lies in our capacity to unconditionally value all insights across the global South and global North (Cross, 2018; Lazarus, 2018, 2019a). For example, "listed in the prevalence of cybercrime perpetrators, Nigeria, the United Kingdom, and the United States are at the top of the FBI's league-table"[1] (Ibrahim, 2016, p.44). Nigeria, arguably, is not less significant than nations from the global North. Therefore, as Cross's (2018) work pointed out, the inclusion of Nigerian scholars' narratives is central and necessary to discussions about cyber-fraud, not least because they provide invaluable layers of explanation regarding the cultural dimensions of cyber-fraudsters. One way to rectify this type of omission is to mobilise literature about Nigerian culture that interacts with cyber-fraud presently missing in the mainstream narratives (e.g. the lens of "digital spiritualization", Lazarus, 2019a, p. 3–5). Such aspects of Nigerian culture are "critical to building a more effective and holistic approach to target online fraud, not only within Nigeria but worldwide" (Cross, 2018, p. 261). Based on the preceding insights, this article relies on marginal voices more than the broader body of research on cybercriminals.

While what constitutes cybercrime issues in most Western nations such as the UK and the US may involve many aforementioned types of cybercrime, the meaning of cybercrime in Nigeria is fundamentally rooted in socio-economics (Ibrahim, 2016). Therefore, in critiquing the dominant cybercrime classifications, Ibrahim (2016, p. 55), despite lacking primary empirical data, argued that "the conceptual 'pipelines' of the cybercrime in the Global North may not hold water in Nigeria." While one might be inclined to suggest that a broader canon of cyber-fraud (e.g. Button and Cross, 2017; Howard, 2009; Schoepfer et al., 2017) is needed in research on the cultural accounts of the agency of social control on cybercriminals, our strategy is based on the principles of cultural relativism. This strategy connects with the belief that one cannot impose meanings on another culture or context as each situation must be understood from the inside (Beirne, 1983; Ribbens McCarthy and Gillies, 2018). This strategy also connects with the belief that there are no "universal" "truths" about the contextual contours of digital crimes such as cyber-fraud (Ibrahim, 2016; Lazarus, 2019a). Accordingly, this current study goes in searches of "local truths" about cybercriminals through the lens of law enforcement officers on the ground in Nigeria.

Monetary benefits are central to the meaning of cybercrime in Nigeria, popularly referred to as "419 fraud" (e.g. Ibrahim, 2016; Igwe, 2007); historically, 419 is derived from section 419 of the Nigerian Criminal Code dealing with fraud. Though there are many types of cyber-fraud (Button and Cross, 2017; Schoepfer et al., 2017), here we examine multiple variations of Advance Fee Fraud (AFF) or 419 (Igwe, 2007; Rich, 2017; Whitaker, 2013). AFF is a confidence trick in which victims (e.g. victims of romance scams) are deceived into advancing relatively small sums of money in the hope of realizing a much larger gain (Chang, 2008; Rich, 2017; Whitaker, 2013). This form of fraud (AFF or 419) is embedded in Nigerian history because they are social products and the term is directly coined from section 419 of the code. The online versions of AFF are locally known as "Yahoo-Yahoo" (e.g. Adeniran, 2011). The term "Yahoo-Yahoo" was coined based on the dominance of Yahoo emails, apps, and instant messaging in perpetrator–victim communications in the mid-2000s (e.g. Trend Micro and INTERPOL, 2017) during the Internet boom in Nigeria. The perpetrators of "Yahoo-Yahoo" were hence popularly called "Yahoo-boys" (e.g. Aransiola and Asindemade, 2011).

2.3. Yahoo-boys and cultural cues

The term "Yahoo-boys" signifies that the perpetrators of the infamous "Yahoo-Yahoo" are predominantly male (Lazarus, 2018, p. 67). The use of emails served as the initial communication phase for some Yahoo-boys, and many victims have been deceived and defrauded all over the world (EFCC, 2018; Whitaker, 2013). Rich's (2017) comprehensive content analysis of a large corpus of AFF emails is revealing (see also Chang, 2008). These researchers observed that authors of AFF emails commonly use a "trust rhetoric" (e.g. Rich, 2017) and "authoritative and urgent" language (e.g. Chang, 2008) to defraud their victims. This body of research (e.g. Adogame, 2009; Chang, 2008; Rich, 2017) sheds light on cyber-fraudsters and their art of persuasive language. However, in recent years, "Yahoo-Yahoo" has shifted from merely sending multiple emails to unsolicited recipients to the targeting and befriending of victims on dating websites or Facebook (EFCC, 2018). While Yahoo-boys generally prefer victims from foreign nations with high currency value (Akanle et al., 2016), remarkably, most victims of Yahoo-boys are swindled in the context of "love" and "friendship" with charms and magic (Lazarus, 2019a). Because "love" and "friendship" are specific aspects of "Yahoo-Yahoo" narratives (Lazarus, 2018), victims' plights are not only financial but also psychological (e.g. Cross et al., 2018; Ibrahim, 2016; Sorell and Whitty, 2019). Yahoo-boys control their "clients" (victims) with various spiritual means, such as invoking of spells on victims' photographs in shrines and communicating with them through words-of-power (locally known as "*do as I say*") on the telephone (Lazarus, 2019a). "*Do as I say*" spells or "words-of-power [can] unlock cosmic forces that can make the spiritual manifest into the physical" and, in this way, spells can be invoked or undone by words-of-power (Peavy, 2016, p. 101). While it may be critical to investigate the symbolic roles of love potions and the mystical powers that can make the spiritual manifest into the physical, there is a dearth of research on Yahoo-boys and the occult economy.

[1] However, a critical perspective has pointed out that the statistics the FBI relied upon to inform the state of cybercrime perpetrators across nations, even when they represent the underlying reality, are socially and selectively constructed (Ibrahim, 2016, pp. 50–52).

Accordingly, some interview studies refer to cybercriminals who defraud their victims with supernatural powers as "Yahoo-boys plus" (e.g. Melvin and Ayotunde, 2010; Tade, 2013). These prior studies (e.g. Melvin and Ayotunde, 2010) noted that only a group of cybercriminals make use of magic/spiritual powers to defraud victims, whereas no study has extended this implicit classification beyond this method of operation. This article sets out to fill this gap. The bottom line is that like some law-abiding Nigerians, the cybercriminals (Yahoo-boys) find the use of magical powers meaningful (Lazarus, 2019a) as exemplified in popular music. A recent study on the representations of Yahoo-boys in hip-hop music suggests that "Yahoo-Yahoo" embodies the occult economy (Lazarus, 2018). Nowhere is the link between the occult economy and Nigerian hip-hop music more evident than in Kelly Handsome's song which depicted Yahoo-boys as follows:

> "…Maga don pay/Mugu don pay/shout hallelujah…/…hallelujah owo…/…/…hallelujah ego…/… hallelujah, hallelujah kudi, kudi../I don suffer, but I now don hammer, papa God don bless me, no one can change it…/…
> ("The gullible has paid, the senseless has remitted/ shout hallelujah…/…hallelujah, hallelujah money…/…hallelujah, hallelujah money…./…/ hallelujah, hallelujah money, money…I have suffered a lot, but now I have hit the jackpot, Almighty God has blessed me, [and] no one can change it")" (Lazarus, 2018, p. 73).

The above song attributes the aquisition of wealth to "real or imagined" spiritual powers, but that is not all. While this prior study (i.e. Lazarus, 2018) noted that cybercriminals and musicians are connected, it has homogenised these cybercriminals as a single group. Bearing this in mind, this current study aims to bifurcate the characteristics of these criminals beyond the use of magical powers. Nonetheless, it is also remarkable that this type of lyrical representation shows that Yahoo-boys glamorize cyber-fraud.

So, while some researchers implicated poverty and/or unemployment as the causes of cyber-fraud among Nigerian youths (e.g. Adesina, 2017; Akanle et al., 2016), other researchers have pointed out that conspicuous consumption (Ibrahim, 2017; Ojedokun and Eraye, 2012) and masculinity or "doing gender" (e.g. Lazarus, 2019b; Smith, 2017) are also fundamental to the discussion of "Yahoo-Yahoo." Since "Yahoo-Yahoo" is primarily motivated by monetary rewards and most Yahoo-boys implicated in such crimes have no employment records (EFCC, 2018), it is reasonable therefore to concede that crime may be one of the Yahoo-boys' ways of "doing gender, when legitimate means of demonstrating their masculinity are denied" (Lazarus, 2019b, p.10; see also Messerschmidt, 1993; West and Zimmerman, 1987). For symbolic interactionists (Carter and Fuller, 2016; West and Zimmerman, 1987), the concept of "doing gender" demonstrates the socially constructed nature of masculinity as developing out of repeated, patterned interaction and socialization processes.

Accordingly, cultural expectations of masculinity and femininity "perpetuate heterosexual male-domination over women" (Connell and Messerschmidt 2005, p.832) and, in Nigeria, men (and boys) are socialised to be sole bread-winners and the principal head of the household (Eboiyehi et al., 2016; Ibrahim, 2015; Smith, 2017), which increases their financial responsibilities as Lazarus (2019b) noted. On the flipside, women's possession of high economic power can have detrimental effects on their marriages and their chances of remarriage in Nigeria (Lazarus et al., 2017). Indeed, gender is a central source of social disadvantages that positions these women between exclusion and belonging (Lazarus, 2019b). "In virtually every arena of Nigerian men's lives, money's value is closely tied to the social work that it does in men's relationships with women" (Smith, 2017, p. 160). Since gender-category membership is attached to the cultural expectations and performativity (Connell and Messerschmidt 2005; West and Zimmerman 1987), in this context, "men's cultural positionality in society influences them to be generally more 'desperate' to achieve financial success than women online" by any means possible such as cyber-fraud (Ibrahim, 2016, p.54). So, the meaning "wealth" has for men in relation to women may be related to the predomination of young men being involved in "Yahoo-Yahoo." Cultural contexts in Ngeria "serve as a resource for understanding gender and crime connections, and offer additional layers of explanation" (Lazarus, 2019b, p.10). These cultural forces resonate with the view that gender is constructed through interaction and that men and women are culturally assessed for their gender performances in both interactional and institutional contexts (Carter and Fuller, 2015; West and Zimmerman, 1987). Closely related to the above are the expectations of people in tertiary institutions and the associated consequences.

Dominant perspectives further suggest that education increases the returns to legitimate work, and legitimate work generally raises the opportunity costs of offending (e.g. Lochner, 2004; Machin et al., 2011). However, university education does not by itself provide an automatic ticket to conventional employment or economic stability in Nigeria (Ibrahim, 2016). Even if a graduate secures legitimate employment, many conventional occupations leave workers vulnerable to financial predicaments that imperil their capacity to provide for themselves and their dependents (Smith, 2017). In these contexts, research on cybercriminals in universities has demonstrated that young adult male Nigerians, mainly university students/graduates, constitute the bulk of cyber-fraudsters (e.g. Aransiola and Asindemade, 2011; Ojedokun and Eraye, 2012; Tade, 2013; Tade and Aliyu, 2011). While one may be inclined to point out that the selective sample of these studies (i.e. solely university students) may have shaped their findings, Ibrahim's (2017) interview study, which explored the views of 17 Nigerian parents, agreed with the above authors. A more critical issue is that as Helfgott (2013) and Payne (2018) noted, researchers value using a categorisation approach to studying crime and criminals. Such an approach, for example, helps to map out 'links between different types of behaviors within specific crime categories' (Payne, 2018, p.18). "Knowing the social and situational-contextual factors that distinguish particular categories of criminals is crucial to theoretical understanding and policy practice" (Helfgott, 2013, p.21). However, no study has considered classifying the Nigerian cybercriminals on the basis of critical themes in literature such as musicians-cybercriminals linkages and university education. To fill this gap (and extend the existing classification beyond the issue of spirituality as previously mentioned), it is critical to explore the narratives of the Economic and Financial Crimes Commission (EFCC) frontline agents. As far as this current study is concerned, no study has sought the narratives of the Economic and Financial Crimes Commission (EFCC) frontline agents (or law enforcement officers for that matter) regarding Yahoo-boys.

2.4. The EFCC

The EFCC was established in 2002 primarily to deal with all "corruption issues" in Nigeria (Obuah, 2010; Pierce, 2016), as corruption is a complex social, political, and economic phenomenon that affects all countries (UNODC, 2017). Some researchers claim that, in Nigerian society, political impunity, bribery, and corruption have created a social environment in which fraudulent practices are normative for ordinary Nigerians (Pierce, 2016; Smith, 2008). Therefore, the EFCC was established to serve as a national coordinator for investigating money laundering and other economic crimes (Obuah, 2010; Pierce, 2016; Umar et al. 2016). Regional policy responses to crime problems are the concerns of international communities (Newburn and Sparks, 2004) and the concerns of international communities in particular played a role in motivating the Nigerian government to set up the EFCC (Obuah, 2010; Umar et al. 2016) and update its laws. Nigeria enacted the 2015 Cybercrime Act to "provide an efficient and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria" (Cybercrime Act, 2015).

The EFCC is the law enforcement agency that investigates and prosecutes financial and economic crimes such as AFF, corrupt practices, illegal bunkering, tax evasion, and all aspects of money laundering in Nigeria (UNODC, 2017). No human organization is perfect, however, and there are often corrupt officials within law enforcement institutions (Reiner, 2010). For example, some researchers have implicated prominent politicians in using the EFCC as tools to oppress and intimidate their political opponents (e.g. Adeniran, 2011). Despite such challenges, the EFCC has been acknowledged in general academic research (Pierce, 2016; Umar et al. 2016) and media discourse (The Nation, 2017) as having had substantial achievements and "zero tolerance for corruption and fraud." In 2017, it was reported that the agency had secured 340 convictions in six months and recovered millions of dollars (e.g. The Nation, 2017). Also, until the creation of the EFCC, law enforcement in Nigeria had been exclusively focused on crimes of the powerless, such as the youth, rather than the powerful, such as corrupt bankers (Pierce, 2016). Indeed, "the creation of the EFCC in Nigeria marked a significant shift from rhetoric about fighting corruption, fraud and money laundering to actually fighting these types of crimes" (Obuah, 2010, p. 24). Since the EFCC is the principal law enforcer of 419 fraud/AFF, the narratives of the frontline EFCC agents will, in Polkinghorne's (1988, p. 19) words, "serve as a lens through which the apparently independent and disconnected elements [of cyber-fraudsters] may be seen as related parts of a whole" (see also Longo, 2015). While many studies have benefited from the interactionist perspective, as Carter and Fuller (2015) noted, no study on cybercrime has used the interactionist perspective in a Nigerian context as far as this research is concerned. This study goes in search of the empirical traces of "culture in action" (Swidler, 1990). Consequently, it will benefit from the symbolic interactionist basic premises, based on the above discussions (e.g. masculinity, occult economies, and local worldviews).

3. Theoretical background

This study will benefit from the symbolic interactionism position, which rests on the three premises of Blumer's (1969b/1998, p. 2) original formulation. The first premise is that the meanings that the things and social objects (persons) have for people are the basis of their actions. The second premise is that these meanings are derived from social interactions. The third premise is that these meanings are modified in the process of interaction of individuals over time. There is no objective viewpoint for the critique or compliment of an "immoral" act (Becker, 1967/1997; Reiner, 2016). Indeed, 'people's experience of the world is always mediated by culturally defined meanings, which, although adopted by their personal experience, condition how and what they conceive as reality in their narratives' (according to symbolic interactionist perspectives) (Longo, 2015, p. 34). Arguably insights from symbolic interactionist perspectives will be useful to make sense of the narratives of officers regarding cyber-fraudsters (fellow Nigerians).

4. Methods

4.1. Participant description and interview data

This study sought the views of EFCC officers concerning Nigerian cyber-fraudsters (Yahoo-boys) and their operations. To explore the narratives of law enforcement officers regarding Yahoo-boys, 40 EFCC officers (70% male and 30% female) from two Nigerian cities (Abuja & Lagos) were recruited. While many agents of state apparatus have been implicated in corrupt practices (Ibrahim, 2017), EFCC officers strive to draw a clear line between the agency and corrupt institutions in Nigeria (Umar et al., 2016). In this context, EFCC officers, if interviewed by "outsiders" outside the agency, could, for example, easily be accused for "passing sensitive information to outsiders" for material gains. This explains why, to date, to the best of our knowledge, no one has been able to access this "hard-to-reach data." However, we circumvented this practical problem by adopting an innovative strategy.

Because one of the authors is an EFCC officer as well as a researcher, the authors were able to access the "impossible" data set. The involvement of the officer as a researcher (i.e., "insider-researcher") facilitated access negotiations with other gatekeepers and helped the research team to develop a high level of rapport with the interviewees. The establishment of rapport between a respondent and the interviewer, or lack thereof, is a critical aspect of the interviewer gaining the respondents' cooperation to complete a meaningful interview. Also, because the interviewer and interviewees were members of the agency (EFCC), they were able to harness a deep, in a Weberian term, "verstehen" (understanding) of their roles while having open and engaged discussions on topics that may not have been otherwise possible. While interviews are products of social encounters involving co-construction, mutual agreement, and trust (Morris, 2018; Ribbens, 1989), the "insider-researcher" emphasized confidentiality/anonymity and informed fellow officers that the study was to gather data for academic research on the subject.

To increase the level of rapport between the interviewer and the interviewees in this study, the "insider-researcher" recruited and individually interviewed fellow officers (70 to 80 minutes each). All officers were interviewed in the EFCC headquarters in Abuja, with the officers based in Lagos being interviewed during their various assignments in the headquarters. Involvement in the study was formalized through the obtaining of the interviewees' consents for the interview. Officers (interviewees) were asked about their experiences with offenders, particularly the cybercriminals' characteristics. The importance of sharing their thoughts about cyber-criminals with a fellow officer who was also a researcher appears to have encouraged the participants to consent to the interviews. Gathering data from law enforcement officers about criminals is consistent with prior research such as Hutchings and Chua's (2017) study which interviewed Australian police officers. In-depth, semi-structured interviews were used, and all interviews were tape-recorded and transcribed verbatim. The selection criteria were that the officers had at least four years of work experience as a frontline law enforcement agent and at least a university degree.

These officers were considered to be appropriate interviewees for our study because they had worked on a significant number of cases regarding cyber-fraudsters according to EFCC's (2018) records. Participants ranged in age from 27 years to 52 years, and their work experience ranged from five to 14 years. A total of 26 frontline investigators and 14 frontline prosecuting lawyers were interviewed between September 2017 and January 2018. While the investigating officers routinely interview complainants and suspects, including Yahoo-boys, they also interrogate them when necessary. Additionally, they give testimony in court for the prosecuting counsel (lawyers). The lawyers (prosecutors) are responsible for crime-data synthesis and prosecuting EFCC cases, including cyber-fraud. The reason for their inclusion was that lawyers' courtroom experience in cyber-fraud cases might complement that of the investigators in generating a rich data set. Enhanced by in-group trust and rapport, the interviewees, due to the role that the "insider-researcher" played as the interviewer and an EFCC officer, provided significant insights into the topic. Given that our data would have been almost "impossible" to reach without the interviewer's in-group membership, we believe that the data we present in this study is priceless. Data was subjected to the principles of a directed approach to qualitative content analysis (DAQCA) (Hsieh and Shannon, 2005).

4.2. Identification of themes and coding of data

In line with DAQCA (Hsieh and Shannon, 2005), data were coded and analyzed as follows. First, coding began with reading the transcripts and highlighting all text that, on first impression, appeared to represent critical aspects of the materials gathered. The next step in the analysis was to code all the highlighted passages using predetermined codes, because "the goal of a directed approach to content analysis is to validate prior research or theory" (Hsieh and Shannon, 2005, p.1281). So, we derived the sensitising concepts from the main themes of the literature review: [1] "socio-demographic and gender," [2] "spiritual dimension of cyber-fraud", [3] "university students/graduates," and [4] "popular music and cyber-fraud connections". These themes served as an initial and subsequent framework to highlight and recognise themes from the data, as suggested by Hsieh and Shannon (2005). While the above four themes identified in the literature were the high-level codes we used, these themes intertwined with our empirical data. Because different coders may vary in their interpretation of the text's content, inter-coder reliability is essential (Hruschka et al., 2004; Hsieh and Shannon, 2005). Accordingly, two researchers independently coded the data. While one researcher coded the whole data, the other (i.e. insider-researcher) reviewed 30% of the data set with the same codes from the literature review (previously mentioned). The degree of similarities between both coders was 98%. It is conceivable that DAQCA has some inherent limitations in that researchers have approached the data with an informed but unintended bias to some extent. The researchers, however, "tested" to see if these themes outlined in the literature and background information appeared as expected. Also, most respondents (n = 34) went straight to the main themes in the existing literature such as "male domination of cybercrime," in their first response without further probing questions. The following is an example of the first interview question:

> Interviewer: "My first question is, based on your experience as a law enforcement officer, how do you describe or define the main perpetrators of cybercrime in Nigeria?"
> Respondent (over five years of experience): "Oh, you mean the boys that normally go to the Internet to defraud people?"

This type of dialogue suggests that the core limitation of a DAQCA did not have a substantial negative effect on the findings. All direct quotes presented below represent widely shared beliefs of the social control agents interviewed involving the following findings: social-demographic features; the bifurcation of Yahoo-boys; and masculinity and material wealth. These are discussed sequentially below.

5. Findings and discussions

5.1. Socio-demographic features

All interviewees (n = 40) reported that Yahoo-boys are predominantly young male university students and graduates. However, 30 participants reported that the socio-demographic features of these cyber-fraudsters are diverse and include people from affluent, poor, Christian, and Muslims backgrounds. For example, in the words of one prosecutor (over 10 years of experience):

> "I can say concerning the perpetrators of cybercrime really, I think there are certain stereotypes that are there, which may not necessarily be the truth. We expect that every Yahoo-boy is that somebody [paused], even the idea that you call him a Yahoo-boys paints an image in your mind that he is a young man, university educated, conversant with the computer and internet, but it is not normally the case... based on my experience as a law enforcement agent, I can say that regardless of economic background or tribe

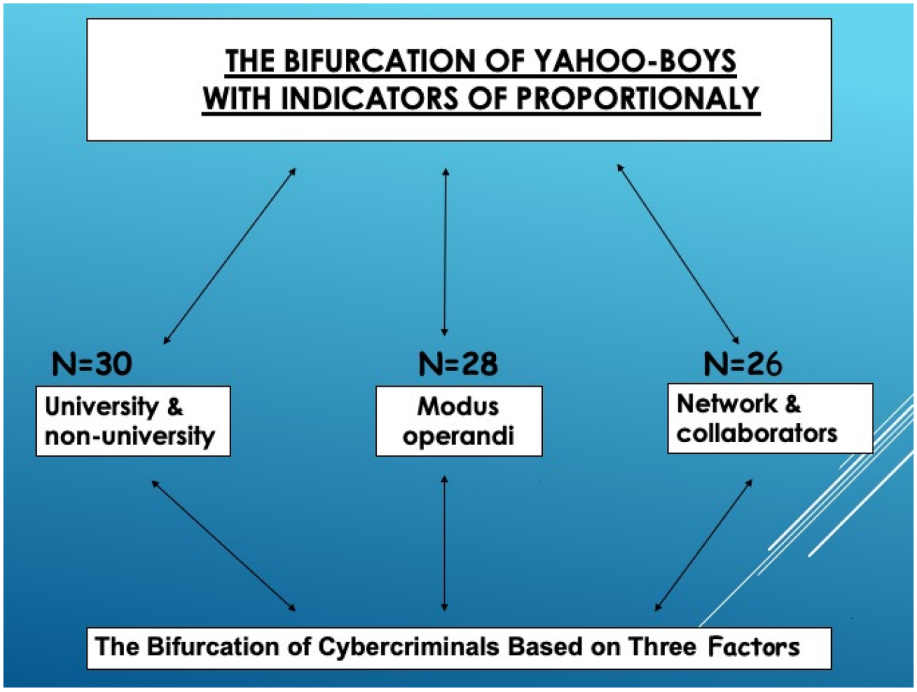


Fig. 1. . The bifurcation of Yahoo-boys with indications of proportionality.

or religion and all that, any ye-ye person [good-for-nothing person] who wants to make it fast in Nigeria goes into internet fraud. Number one, the internet gives anonymity, and low risks. You know, because no police or army checkpoints are online [because no perfect security online]. Secondly, the Internet is a flow, no boundary. It gives you access to people [victims] in real time, quick, quick ... there's no barrier online, and for example, they don't need a visa to talk to somebody in the UK."

Notably, the last sentence is reminiscent of Wall's (2007, p. 185) observation that life online has the capacity for distributing "peer to peer networking and a panoptic gaze that creates an asymmetric ability to enable one person to simultaneously reach many." Equally, despite the idea the there is no clear boundary between cyber-fraudsters and non-cyber-fraudsters, interviewees (n = 40) stated that, based on their experiences on frontline duties as EFCC officers, cyber-fraudsters are exclusively "young" males. It is noteworthy that the chronological meaning of "age" as the dominant benchmark for the definition of "youth" does not hold true across cultures (e.g. in Nigeria). The determinants of "youthhood" in a Nigerian context transcend age and encompass multiple cultural dimensions such as political affiliation and positionality as well as marital status. The underlying idea is that, while some Nigerian researchers have implicated "youths" as responsible for the bulk of cyber-fraud originating from Nigeria, some of these researchers (e.g. Jegede et al., 2016) use the cultural meaning of "youth/age" rather than the chronological meaning because they also include people above 30 years of age as "youths." In fact, critical perspectives suggest that the meanings of youthhood are not constituted similarly across cultures (e.g. Cain, 2000). Therefore, it is conceivable that the meaning of "young men" or "youths" in Nigeria is culturally constructed and must be read in terms of the definitions they carry in a Nigerian context.

5.2. The bifurcation of Yahoo-boys

Apart from the demographic characteristics of Yahoo-boys, some respondents divided Yahoo-boys into two main groups (Yahoo-boys-digital and Yahoo-boys-analogue) based on their experiences as frontline law enforcement officers. As shown in Fig. 1, the bifurcation of Yahoo-boys was not only based on educational background (n = 30), as previously noted, but also included other characteristics (e.g. "network and collaborators," "modus operandi").

Support for the distinctions between these broad groups of Yahoo-boys in the majority of the officers' reports is exemplified by the following responses:

"The word 'analogue' and 'digital' is just a reference point. Yahoo analogue are those people who are local, opportunists, without a secondary education, they see Yahoo-Yahoo, and they jump into it. If you look at their patterns, they are quite different from those who have passed through universities or those who are fully educated or those who studied info-tech. You see, they are two different sets of people, and their modus operandi, everything, are different. Somebody who just picked up the trade from the street would not be as advanced as somebody who has acquired university education…passed through the educational process … So, they are two different people." (Male investigator with over 11 years of experience)

"The Yahoo-boys-analogue generally sends thousands of scam emails to potential victims. They do it randomly, and pray that some of targets would respond … give them their pictures or send them personal items. They would now work on the victims' photos in shrines to cast spells on them and remove difficulties in controlling and manipulating them for financial purposes. But

the digitally advanced Yahoo-boys, I think, do not rely on *juju* [spiritual/magical powers] a lot. Because they rely on advanced tech to defraud victims. You can even see all these differences when you arrest them and search their apartments. Sometimes, you find a lot of spiritual items, victims photos in private juju alters and some amulets. They [these types of evidence] tell you the type of person you are dealing with." (Male investigator with seven years of experience)

5.2.1. University and non-university education

As previously emphasized, Yahoo-boys can be divided into two broad groups based on education and those who have a university education are quite different from non-university educated Yahoo-boys. Education is the engine of social mobility in modern society, whereby the time people spend in education may limit the time they are available for participating in criminal activities (e.g. Hjalmarsson et al., 2015; Machin et al., 2011). These authors' ideas do not necessarily apply to "Yahoo-Yahoo." The time people spend in Nigerian universities does not limit the time they are available for participating in "Yahoo-Yahoo." Everyone can be an achiever once the skill sets are acquired on the street. However, Yahoo-boys who generally get ahead in "Yahoo-Yahoo" business ventures and are most sophisticated in the "scam game" are the university-educated Yahoo-boys, according to most respondents. Individuals who have higher educational attainment are most likely to have a higher level of connections with the broader body of educated Nigerians in higher socio-economic positions. The higher levels of exposure to the elite group and technological environments may also be related to advanced knowledge and skills in technology.

Similarly, previous research on crime and education linkage has suggested that education can also increase the earnings from crime as specific skills acquired in school may be inappropriately used for criminal activities (e.g. Lochner, 2004; Machin et al., 2011). Yahoo-boys-digital (university-educated cyber-fraudsters) are not only more advanced than those who are non-university educated, they are also more difficult for law enforcement agents to criminalize because in the words of one respondent, "they [Yahoo-boys-digital] are always conducting their own research even more than law enforcement." Like the EFCC in Nigeria, law enforcement agencies in general, even in most advanced nations, as Broadhurst (2006, p. 4) noted, "play catch-up with cyber-savvy criminals." Equally, while one might question why college education may be needed in "Yahoo-Yahoo" business, email scams are saturated with unskilled or average computer users, and technological expertise and English language proficiency are currently needed to succeed in "Yahoo-Yahoo" contexts. A total of 30 participants not only suggested that a large number of university students/graduates and non-university students/graduates are involved in perpetrating cyber-fraud, but they also supported the distinctions between the groups of Yahoo-boys based on the theme: "university and non-university education." For example, according to one investigator (over 11 years of experience):

"The digital Yahoo boys are more advanced. As an investigator, if you are dealing with a Yahoo analogue group, the applications they normally use are the ones you can buy online. But Yahoo-boys-digital, they don't just buy applications online, they've people who design them [Trojan or other malicious software applications] according to their needs. They've their contacts who they can just say, do this and this for me; I want a computer program that can perform this, maybe a Trojan horse that can perform specific duties. He tells the programmer, this is how I want the Trojan to work, behave and all that. Because Yahoo-boys-digital have more analytic minds than Yahoo analogue guys. The digital guy would take his time, study the system, identify weaknesses, think of how to beat the system. So, if you look at the systematic way, you would see that the digital boys are more difficult to catch. And that also indicates that they make more money than Yahoo analogue ones."

It is noteworthy that there is a general consensus in existing studies (e.g. Aransiola and Asindemade, 2011; Jegede et al., 2016; Ibrahim, 2017) that university students and graduates (including dropouts) are the main perpetrators of cyber-fraud that emanates from Nigeria. Similar to existing studies, our current study supports the idea that Nigerian university students/graduates are the major culprits in terms of "Yahoo-Yahoo" business. Unlike extant studies, however, our current study has, through the bifurcation of Yahoo-boys, deconstructed the homogenization of Yahoo-boys as one group under the umbrella of "university students/graduates." As one agent described it, unlike Yahoo-boys-analogue, "the more sophisticated we [agents] become, the more re-organized with their complex syndicates they [Yahoo-boys-digital] become."

5.2.2. Modus operandi

Since some Nigerians believe that true wealth is rooted in the spiritual realm, they view those who have the knowledge to appease the gods and ancestral spirits as being rewarded in material terms (e.g. Lazarus, 2019a). The interviewees (n = 40) mentioned the issue of "spiritualism in cybercrime.", which aligns with the existing interview studies (e.g. Melvin and Ayotunde, 2010). In particular, it was observed that Yahoo-boys-analogue tended to use magic powers more than Yahoo-boys-digital in their attempts not only to defraud victims but also to avoid prosecution. To avoid prosecution here means that these criminals use spiritual/magical powers to [a] increase the chances of their crimes escaping the EFCC officers' surveillance and [b] reduce chances of the EFCC officers investigating their crimes. In a similar vein, Frankle and Stein (2005, pp. 138–139) noted: "many peoples do not distinguish in practice between technological knowledge and magical knowledge. The goals of both are very much the same, and one would be ill-advised to pay attention to one without paying attention to the other."

In a similar vein, the goals of technological knowledge and mystical knowledge in the "Yahoo-Yahoo" context are the same: to maximize benefits; and to avoid prosecution. However, there are notable differences between these two spheres of knowledge. One might argue, as Malinowski (1954/2014, p. 17) pointed out, that "we do not find magic wherever the pursuit is certain, reliable, and well under the control of rational methods and technological processes." Hence, it is conceivable that cyber-fraudsters who rely more on magical knowledge (Yahoo-boys-analogue) than technological knowledge may be facing a less certain situation in "Yahoo-Yahoo"

business than the Yahoo-boys-digital group. It is plausible that higher computer/technology expertise reduces the uncertainty associated with "Yahoo-Yahoo" business ventures such as the trial-and-error scam email format popularly used by the Yahoo-boys-analogue category. Equally, it is conceivable that Yahoo-boys-analogue, facing a technological competition they cannot win (Yahoo-boys-digital group always does), they subscribe to the occult economy to achieve their goals. A more critical issue is that our current study helps to illuminate the specific category of Yahoo-boys that usually depend more on mystical powers in cyber-fraud perpetration that originates from Nigeria. A total of 28 participants supported the distinctions between the groups of Yahoo-boys based on the theme "modus operandi." In the language of one investigator:

> "Yahoo digital depend mostly on 'info tech' ... another thing about Yahoo analogue is that you see most of them dey use *juju* [magical and spiritual powers] to operate [you see, most of them use magical powers to defraud their victims]. In the sense that when they start communicating with you [referring to victims], they would put your picture under their laptop. Even some of them use blood, cut their hand and put the blood on the picture and all that. You see, that is the way of a typical Yahoo analogue guy."

These narratives from the agent support the observation that Yahoo-boys-analogue associate mostly with spiritualists who usually assist clients with their spiritual needs. This category of cybercriminals depends on the spiritualists more than their counterparts (i.e., Yahoo-Boys digital group) which resonates with the view that people do not generally subscribe to magical/spiritual powers wherever the pursuit is certain, reliable, and well under the control of rational methods and technological processes. To put a victim's picture under their laptop symbolizes the spiritual dimension of cyber-fraud because it is a ritualized practice commonly prescribed by spiritualists. After the spiritualist (native doctor) might have "worked on" the picture (cast a spell on it possibly in his/her shrine), it is then necessary and sufficient for fraudsters to simply place the photograph under the computer while chatting/messaging the victims of fraud. Also, in the words of one respondent, "fraudsters also talk to the [victims'] pictures repeatedly" which represent the words-of-power ("*do as I say*" rhetoric), this being a spiritual way of manipulating victims for material rewards. It may be plausible that the "authoritative language" (Chang, 2008) and "trust rhetoric" (Rich, 2017) commonly used by some cybercriminals to communicate with their victims could be linked to "*do as I say*" rhetorical spells or words-of-power. If cyber-fraudsters believe they have spiritual authority over victims, they may be more inclined to deploy excessive "authoritative language" than otherwise. This spiritual worldview illuminates how, and to what extent, the relationship between the spiritualists and Yahoo-boys-analogue is a critical dynamic for the social construction and negotiation of identity and belonging in "Yahoo-Yahoo" contexts. It also illuminates Kalu's (2002, p. 674) idea that some Nigerians could be viewed as "feeding on the red blood corpuscles of the primal world and spiritual shrines in rural areas," as mentioned previously. The spiritual manipulation of victims highlighted here, indeed, urges cyber-fraud researchers "to look beyond normal 'scientific evidence' and consider the traces of spiritual manipulations of victims for material gains that are all too often ignored in 'normal' social science" (Lazarus, 2019a, p.1).

Notably, previous studies (e.g. Melvin and Ayotunde, 2010; Tade, 2013) have explained that Yahoo-boys exploit the spirit world to maximize their chances of success in defrauding victims online and called them "Yahoo-boys plus." While our current study builds on these existing bodies of knowledge, it finds that it may be misleading to dichotomize or homogenize Yahoo-boys solely based on the exploitation of the spiritual world for wealth accusation. The dichotomization of these cyber-fraudsters (Yahoo-boys-analogue and Yahoo-boys-digital) includes other factors such as networks and collaborators in the social domain, which supports the notion that the cyberspace is a mere extension of the indigenous worldviews in Nigerian society.

5.2.3. Networks and collaborators

While Yahoo-boys-analogue associate more with spiritualists than Yahoo-boys-digital, the latter exclusively have connections with new music industries and musicians. In other words, some musicians and Yahoo-Boys 'reciprocally construct the destiny of one another' (Lazarus, 2018, p.74). According to Lazarus's (2018) study, while some musicians and Yahoo-boys are "birds of a feather that flock together", the core aspects of their relationship are based on reciprocal economic benefits and determined by them. This study grouped Yahoo-boys as one group in its analysis of con-artists' and musical-artists' connections, whereas the current study sheds more light on this linkage. Unlike Yahoo-boys-analogue, Yahoo-boys-digital predominantly "club together" with musicians who represent them in their lyrics. For Blumer (1969a), interaction occurs within a particular social and cultural context in which physical and social objects (persons), as well as situations, must be defined or categorized based on individual meanings. Accordingly, the interactions and social intercourses between musicians and Yahoo-boys were critical in what one respondent called the "cybercrime money laundry." And a total of 26 participants supported the distinctions between the groups of Yahoo-boys based on the theme of "networks and collaborators." According to investigators:

> "But for those who are really educated [Yahoo-boys-digital] they invest the money and through that investment, they launder the money. If you look at all these new music industries, most of them are used to launder money. Let me give you an example, if you listen to one music, Oshozondi by Slimcase. Have you heard of it before? [researcher responded, no!]. If you listen to Oshozondi, he listed names of all the popular Yahoo Boys in Lagos. You understand. These are some of the differences [difference between the two groups of cyber fraudsters]." (Agent with over ten years of experience).

> "Let me tell you; almost all the music labels that you see, they are being owned by Yahoo-digital guys. And that is why you need to study what we call, 'cyber money laundering'! … Because people would buy different properties in the name of music industries owned by Yahoo-boys [digital]. They're the ones who have registered music industries to cover the actual fraud that they are doing. They're making it, industry, industry, industry, but if you ask them where do you get the money to establish those companies, all those music industries, they cannot justify it. That's where the cyber money laundering is coming in now." (Agent with 12 years of experience).

It is conceivable that the link between Yahoo-boys-digital and musicians explains why the former (unlike Yahoo-boys-analogue) invest their income in the music industry in Nigeria. The Yahoo-boys-digital also have an extensive network that includes not only bank clerks who may assist ordinary Yahoo-boys-analogue to withdraw fraudulently obtained money without questions, but also hi-tech bankers. One male investigator described the involvement of these bankers in cybercrime money laundering as follows:

> "For every transaction, they [corrupt hi-tech bankers] get 15%. Let me give you an example, like POS [point of sale]. For every POS, there's a particular threshold attached to that transaction. It means that an account is attached to POS, it might say that it cannot receive let's say credit transaction of more than two million a day. Somebody managing the POS programmed from the bank, maybe the network administrator or the application manager. What this boy [Yahoo-boy-digital] would do if he wants to move or receive a larger sum of money; he needs somebody with a company account. Yes? But that company has a threshold, let's say two million or five million. They [Yahoo-boy-digital] now need bankers to activate what we call 'code 002' which is a security dial monitoring the credit of that POS account. So, the IT guy in the bank can switch it off for the fraudulent money to enter. And the money would enter. It would not raise the alarm. You see he [the banker] has aided and abetted crime because he has 15% of the money."

Even if many legitimate occupations leave most workers vulnerable to financial difficulties that imperil their capacity to provide for themselves and their dependents, bankers are not one of the poorest group of workers in Nigeria. Therefore, it is simplistic to assert that poverty may primarily motivate their actions. It is plausible that the corrupt bankers described above were acting toward material wealth on the basis of the meanings their collaborators (Yahoo-boys) have for them. If representative, legitimate institutions aid and abet cyber-fraud to add to their legitimate income streams. It suggests that there is a fine line between the cultural meaning of "Yahoo-boys" and some claiming to be law-abiding Nigerians. As indicated in the above narratives, the seeming boundary between Yahoo-boys and some representatives of legitimate institutions, such as bankers, is blurred because they engage in similar practices that constitute fraud and corruption.

Additionally, based on the above narratives, it is reasonable to deduce that corrupt bankers symbolize a store of value because wealth-in-people (e.g. bankers) could easily translate into wealth-in-money in "Yahoo-Yahoo" contexts. To have strong allies and networks of bankers is arguably a useful asset in the accumulation of wealth in "Yahoo-Yahoo" businesses. Similarly, previous studies (e.g. Aransiola and Asindemade, 2011; Ibrahim, 2017) have indicated that Yahoo-boys collaborate with bankers to maximize their chances of success in "Yahoo-Yahoo." Our current research, however, demonstrates that it is misleading to homogenize Yahoo-boys as a single group with respect to three related features: "university education;" "networks and collaborators;" and "method of operation." Concerning the links between legitimate institutions (banks) and the cyber-fraudsters, while Yahoo-boys-analogue commonly associate with junior bank officers, Yahoo-boys-digital group "club together" with senior bank officers. They generally collaborate with high-level bankers such as network administrators and application managers. The critical point here is that in gift giving (e.g. bribery or "*dash*") the honor of giver and recipient are reciprocally engaged and gift exchanges represent ritualized bonding between the giver and the receiver (Droz and Gez, 2015; Mauss, 1925). While gift exchanges may strengthen the bond between the Yahoo-boys-digital group and high-level bankers, the lack of such exchanges may weaken the bond between high-level bankers and Yahoo-boys-analogue and limit their chances of "moving up the ladder" (social mobility in criminal career), given that collaborators are the integral part of "Yahoo-Yahoo." What is less distinguishable among Yahoo-boys is their lifestyle; we found that they generally live extravagant lifestyles, which supports previous studies (e.g. Ojedokun and Eraye, 2012). The above issue (extravagant lifestyles) deserves a closer examination.

5.3. Masculinity and material wealth

Masculinity develops out of repeated, patterned interaction and socialization processes (West and Zimmerman, 1987). Men are culturally socialized to be the head of the household in economic terms and are expected to translate economic power into social prestige from time to time (Ibrahim, 2017; Smith, 2017). For example, a Nigerian man who has economic power, irrespective of his age, under customary and Islamic types of marriages, can marry multiple wives (Lazarus et al., 2017). Culturally, even his adultery is often seen in society as a prestigious act (Chinwuba, 2015; Smith, 2017). A total of 29 officers had a shared belief that men are more culturally expected to have economic power than women; for example, according to a female investigator with 12 years of experience:

> "Our culture is that a man as a man you have to take the girl o-u-t! And when a man has one, two, three of them [women], he has to find means to support them. You see, some married men have concubines. You also see some married men; their religion allows them to marry three, four! So, a man with four wives in a culture where the man has to be the provider, the bait would be much more for him than women whose business it is to receive and look good."

Indeed, the manifestation of conspicuous consumption in Yahoo-boys' lives has to be understood as a masculinity performance. The cultural and social positionality of Nigerian men as reported above resonates with Lazarus's (2019b, p.10) position that "men's hegemonic role in cyber-fraud as perpetrators is the mirror of, and made possible by, women's subordinate posity in society". 'In virtually every arena of Nigerian men's lives, money's value (and its stigma) is closely tied to the social work that it does (or fails to do) in their relationships with other citizens' (Smith, 2017, p. 160). Young men generally affix their aspirations on material wealth and "assemblage of goods," to live a meaningful life according to the dictates of the Nigerian society (Ellis, 2016). When a man spends money on occasions such as his parents' burial rites, girlfriends' parties or wedding ceremonies, "part of what he is doing is converting wealth into prestige" (Smith, 2017, p. 210). In Blumer's (1969b/1998, p. 4) words, "[T]he meaning of a thing for a person grows out of the ways in which other persons act toward the person with regard to the thing." Thus, "doing gender" for Yahoo-boys is unavoidable because gender-category membership is attached to the allocation of power and cultural expectation for men to generate

wealth (almost by any means necessary). Accordingly, the symbolic meaning of material wealth here underscores that it embodies not only a mechanical reflection but the imputed sentiments.

For Cooley (1909/1998), the thing that moves us to our pride or our shame is not the mere mechanical reflection of ourselves, but an imputed sentiment and the imagined effect of this reflection upon another's mind and society. Given the socially constructed nature of masculinity as developing out of repeated, patterned interaction and socialization processes (West and Zimmerman, 1987), the seemingly obvious officers' narratives on Yahoo-boys are far from straightforward. The Yahoo-boys' actions in the virtual world must be read in the light of cultural cues on wealth generation and masculinity as well as the glamorization of wealth in the broader Nigerian society. The social communities of Nigeria glamorize wealth irrespective of the source of the wealth (e.g. Adeniran, 2011; Ibrahim, 2017; Lazarus, 2018). The fraudulent actions of Yahoo-boys are even glamorized in Nigerian popular music (Lazarus, 2018). This reinforces the notion that life online is a mere extension of life in society (e.g. Lazarus, 2019b; Mumporeze and Prieler, 2017).

6. Conclusion

While this study has examined the intersections between cultural factors and information and communication technologies, it is the first study to explore the narratives of EFCC officers in bifurcating Yahoo-boys and their operations. While prior studies, for example, indicated that only a group of cybercriminals deploy spiritual and magical powers to defraud victims (i.e., modus operandi), our study has extended this classification into more refined levels in its bifurcation of cybercriminals. 'Distinguishing between categories of criminals is critical to theoretical advancement, policy and practice' as Helfgott (2013, p.21) reminded us. In particular, the narratives of officers have provided insights which may help various local and international agencies [a] to understand the actions/features of these two groups of cybercriminals better and develop more effective response strategies; and [b] to appreciate the vulnerabilities of their victims better and develop more adequate support schemes. Indeed, insights from our study could help various local and international agencies, as well as social scientists around the world, to understand the actions/features of these two groups of cybercriminals better (as illustrated in Fig. 1). One might also be inclined to suggest that, for example, these insights may help relevant agencies in understanding the best strategy to reduce the occurrences of these crimes. By benefitting from the basic premises of the interactionist position, this study has proposed that, since indigenous worldview and masculinity emerge out of repeated, patterned interaction and socialization processes, "Yahoo-Yahoo" may be one of the ways these Yahoo-boys construct their culturally expected identity regarding wealth acquisition in society. Because of this, we believe insights from this research have implications for the value of the interactionist perspective in making sense of crimes on the Internet. Unlike the existing studies on Yahoo-boys, our study has found evidence to deconstruct the homogenization of these cyber-fraudsters as one group (e.g. with respects to "educational attainment" and "networks/collaborations"). Specifically, it has instead proposed rather dualistic groups based on three factors (educational attainment, modus operandi, networks and collaborators) that shed fresh light on a range of prevailing perspectives on Yahoo-boys.

First, there is consensus that young male university students/graduates are predominantly the perpetrators of cyber-fraud (e.g. Adeniran, 2011; Aransiola and Asindemade, 2011; Ibrahim, 2017); the current study, however, demonstrates that a considerable number of non-university students are also involved in perpetrating cyber-fraud. Second, prevailing studies identified that some Yahoo-boys use magical/spiritual powers to defraud victims (e.g. Melvin and Ayotunde, 2010; Tade, 2013). Like these previous studies, the current study indicates that a group of these cybercriminals (Yahoo-boys-analogue) depends more on spiritual powers for their "Yahoo-Yahoo" business than others (Yahoo-boys-digital). Unlike the prevailing studies, the current study also indicates Yahoo-boys can be divided with respect to other attributes: "university education;" "networks and collaborators;" and "method of operation." Third, while our study concurs with research that suggests Yahoo-boys live extravagant lifestyles (e.g. Ojedokun and Eraye, 2012), the current study has additional contributions. First, it explains that, although most Yahoo-boys live a lavish lifestyle, a group of them (Yahoo-boys-digital) invest their illicit income predominantly in legitimate businesses, such as the music industry. Second, it notes that a conspicuous lifestyle for male Nigerians in itself is a mere reflection of gender nuances in society.

While our study provides valuable contributions to the existing body of knowledge, it should be viewed in light of a few fundamental limitations. Its primary weakness is that it offers only a top-down view of a selected group on Yahoo-boys. The perspectives of some frontline enforcers of the law on criminals, as Reiner (2016) noted, are commonly susceptible to prejudice, given that the human narratives about their fellow men/women are culturally defined. "People's experience of the world is always mediated by culturally defined meanings, which, although adopted by their personal experience, condition how and what they conceive as reality" (Longo, 2015, p. 34) as previously mentioned. Equally, we acknowledge the potential dangers of using interviews with social-control agents to discuss offenders because some of them may not (and often do not) have the full picture of the criminals. Additionally, caution should be applied in the interpretation of the officers' narratives concerning Yahoo-Boys and their activities. This is because, we cannot escape the conclusion that all interviews, and interview data, as Morris (2018) and Ribbens (1989) observed, are socially constructed and are products of social encounters within a particular social structure.

The above limitations by no means undermine the importance of this study's main achievement: the bifurcation of Yahoo-boys. Our analyses have helped to propose that these cybercriminals can be grouped into two main categories, based on the multiple axes of differentiation discussed. In Nigeria, "cybercrime" may be fundamentally rooted in socioeconomics (Ibrahim, 2016; Ojedokun and Eraye, 2012) and indigenous worldviews within the occult economy (Melvin and Ayotunde, 2010; Tade, 2013). Indeed, online behaviors are mere reflections of the symbolic meaning and consequences of social products (e.g. the occult economy and the prestige of material wealth) and social actors such as the Yahoo-boys, corrupt bankers, and spiritualists. By implication, the different "business associates," as well as preferred methods of operations of Yahoo-boys-digital and Yahoo-boys-analogue, reinforce the idea that life online is an extension of life offline, reflecting contextual and cultural nuances (Lazarus, 2019b; Mumporeze and Prieler, 2017; Powell et al., 2018).

This article has therefore proposed that, since the occult economy and masculinity develop out of repeated, patterned interaction and socialization processes, cyber-fraud may be one of the ways Yahoo-boys and their associates construct culturally expected identities in society. This, in particular, may be responsible for rendering fraudulent practices acceptable career paths for Yahoo-boys and some representatives of legitimate institutions. Since Yahoo-boys defraud a multitude of victims globally, as Cross (2018) and Lazarus (2018, 2019a) suggested, a better understanding of this phenomenon lies in our capacity to unconditionally value all insights across the global South and global North.

Author contribution statements

[a] **S.L**. conceived & designed the study. [b] **G.U.O**. recruited & interviewed the participants. [c] **S.L**. analyzed & interpreted the data. [d] **G.U.O**. verified the interpretation of data. [e] **S.L**. drafted the whole article. [f] **S.L**. carried out the critical revisions of the article. [g] **S.L.** & **G.U.O**. read & approved the published version.

Acknowledgements

The authors thank all the participants who gave their time and shared their stories. The authors are fully responsible for the views expressed in this article: the article does not represent the views of the authors' institutional affiliations.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.tele.2019.04.009.

References

Adeniran, A.I., 2011. Café culture and heresy of Yahooboyism in Nigeria. In: Jaishankar, K. (Ed.), Cyber criminology: Exploring internet crimes & criminal behaviour. CRC Press, New York.
Adesina, O.S., 2017. Cybercrime and poverty in Nigeria. Can. Social Sci. 13 (4), 19–29.
Adogame, A., 2009. The 419 code as business unusual: Youth and the unfolding of the advance fee fraud online discourse. Asian J. Social Sci. 37 (4), 551–573.
African Development Bank, 2018. 'African Development Bank reported in 2018 that about 78% Nigerians live on less than $2 daily', retrieved: https://www.concisenews.global/business/150m-nigerians-live-on-less-than-2-daily-afdb/, accessed, 28/02/18.
Akanle, O., Adejare, G.S., 2018. Contextualizing pentecostal gatherings in southwestern Nigeria: Social drivers and significance. In: Religion in Context. Nomos Verlagsgesellschaft, Baden-Baden, pp. 145–158.
Akanle, O., Adesina, J.O., Akarah, E.P., 2016. Towards human dignity and the internet: the cybercrime (yahoo yahoo) phenomenon in Nigeria. Afr. J. Sci. Technol. Innov. Development 8 (2), 213–220.
Aransiola, J.O., Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychol. Behav. Social Networking 14 (12), 759–763.
Bae, S.M., 2017. The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. Children Youth Services Rev. 78, 74–80.
Becker, H., [1967]1997. Outsiders: Studies in Sociology of Deviance. New York, NY: Simon and Schuster.
Beirne, P., 1983. Cultural relativism and comparative criminology. Contemporary Crises 7 (4), 371–391.
Blumer, H., 1969a. Symbolic Interactionism: Perspective and Method. Prentice Hall, Eaglewood Cliffs.
Blumer, H., 1969b/1998. Symbolic Interactionism: Perspective and Method. Berkeley: University of California Press.
Broadhurst, R., 2006. Developments in the global law enforcement of cyber-crime. Policing 29 (3), 408–433.
Button, M., Cross, C., 2017. Cyber Frauds, Scams and Their Victims. Taylor & Francis, New York.
Cain, M., 2000. Orientalism, occidentalism and the sociology of crime. Br. J. Criminol. 40 (2), 239–260.
Carter, M.J., Fuller, C., 2015. Symbolic interactionism. Sociopedia. ISA 1, 1–17.
Carter, M.J., Fuller, C., 2016. Symbols, meaning, and action: the past, present, and future of symbolic interactionism. Curr. Sociol. 64 (6), 931–961.
Chang, J.J., 2008. An analysis of advance fee fraud on the internet. J. Financial Crime 15 (1), 71–81.
Chinwuba, N.N., 2015. Human identity: child rights and the legal framework for marriage in Nigeria. Marriage Family Rev. 51 (4), 305–336.
Comaroff, J., Comaroff, J.L., 1999. Occult economies and the violence of abstraction: Notes from the South African postcolony. Am. Ethnol. 26, 279–303.
Connell, R.W., Messerschmidt, J.W., 2005. Hegemonic masculinity: rethinking the concept. Gender Soc. 19 (6), 829–859.
Cooley, C., [1909] 1998. On Self and Social Organisation. Chicago: The University of Chicago Press.
Cross, C., Dragiewicz, M., Richards, K., 2018. Understanding romance fraud: insights from domestic violence research. Br. J. Criminol. 58 (6), 1303–1322.
Cross, C., 2018. Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In: The Palgrave Handbook of Criminology and the Global South. Palgrave Macmillan, Cham, pp. 261–280.
Cybercrime Act, 2015. 'Cybercrime, Prohibition, Prevention Act', retrieved: https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_2015.pdf, accessed 14/03/18.
Dasgupta, N., Ugur, M., 2011. Evidence on the economic growth impacts of corruption in low-income countries and beyond: a systematic review. London: EPPI-Centre, Social Science Research Unit, Institute of Education, University of London.
Donner, C.M., Jennings, W.G., Banfield, J., 2015. The general nature of online and off-line offending among college students. Social Sci. Computer Rev. 33 (6), 663–679.
Droz, Y., Gez, Y.N., 2015. A God trap: seed plan ng, gi logic, and the prosperity gospel. In: Heuser, A. (Ed.), Pastures of Plenty: Tracing Religio-scapes of Prosperity Gospel in Africa and Beyond. Lang, Frankfurt, pp. 295–307.
Eboiyehi, F.A., Muoghalu, C.O., Bankole, A.O., 2016. In their husbands' shoes: feminism and political economy of women breadwinners in Ile-Ife, Southwestern Nigeria. J. Int. Women's Stud. 17 (4), 102–121.
EFCC, 2018. 'The United Nations Office on Drug and Crime Survey', retrieved: https://efccnigeria.org/efcc/9-uncategorised/2714-efcc-adjudged-most-effective-govt-agency, 13/03/18.
Ekeh, P.P., 1975. Colonialism and the two publics in Africa: a theoretical statement. Comparative Stud. Soc. History 17 (1), 91–112.
Ellis, S., 2016. This Present Darkness: A History of Nigerian Organized Crime. Oxford University Press, Oxford.
Frankle, R.L.S., Stein, P.L., 2005. The anthropology of religion, magic and witchcraft. Pearson Allyn and Bacon, Boston.
Hayward, K.J., Young, J., 2004. Cultural criminology: Some notes on the script. Theor. Criminol. 8 (3), 259–273.
Helfgott, J.B., 2013. Criminal psychology and criminal behavior. In: Helfgott, J.B. (Ed.), Criminal Psychology. Praeger, Santa Barbara, pp. 3–42.
Hjalmarsson, R., Holmlund, H., Lindquist, M.J., 2015. The effect of education on criminal convictions and incarceration: causal evidence from micro-data. Econ. J. 125 (587), 1290–1326.
Howard, R., 2009. Cyber Fraud: Tactics, Techniques and Procedures. Auebach Publications, Boca Raton, FL.

Hruschka, D.J., Schwartz, D., St. John, D.C., Picone-Decaro, E., Jenkins, R.A., Carey, J.W., 2004. Reliability in coding open-ended data: Lessons learned from HIV behavioral research. Field methods 16 (3), 307–331.
Hsieh, H.F., Shannon, S.E., 2005. Three approaches to qualitative content analysis. Qual. Health Res. 15 (9), 1277–1288. https://doi.org/10.1177/1049732305276687.
Hutchings, A., Chua, Y., 2017. Gendering cybercrime. In: Holt, T.J. (Ed.), Cybercrime through an Interdisciplinary Lens. Routledge, New York, pp. 167–188.
Ibrahim, S., 2015. A binary model of broken home: Parental death-divorce hypothesis of male juvenile delinquency in Nigeria and Ghana. In: Royo Maxwell, S., Lee Blair, S. (Eds.), Contemporary Perspectives in Family Research. vol. 9. Emerald Group Publishing Limited, New York, pp. 311–340.
Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. Int. J. Law Crime Justice 47, 44–57.
Ibrahim, S., 2017. Causes of socioeconomic cybercrime in Nigeria. In: IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada, pp. 1–9.
Igwe, C.N., 2007. Taking Back Nigeria from 419: What to Do about the Worldwide E-mail Scam – Advance-fee Fraud. iUniverse, Toronto.
Jegede, A.E., Elegbeleye, A.O., Olowookere, E.I., Olorunyomi, B.R., 2016. Gendered alternative to cyber fraud participation: an assessment of technological driven crime in Lagos State, Nigeria. Gender Behav. 14 (3), 7672–7692.
Jones, M.L., 2018. Ctrl+ Z: The Right to be Forgotten. NYU Press, New York.
Kalu, O.U., 2002. The religious dimension of the legitimacy crisis, 1993–1998. In: Falola, Toyin (Ed.), Nigeria in the Twentieth Century. Carolina Academics Press, Durham, Durham, NC, pp. 667–685.
Kigerl, A., 2012. Routine activity theory and the determinants of high cybercrime countries. Social Sci. Comput. Rev. 30 (4), 470–486.
Kirillova, E.A., Kurbanov, R.A., Svechnikova, N.V., Zul'fugarzade, T.E.D., Zenin, S.S., 2017. Problems of fighting crimes on the internet. J. Adv. Res. Law Econ. 8 (3), 849–856.
Lazarus, S., 2018. Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo boys) and hip hop artists. Criminol. Criminal Justice Law Soc. 19 (2), 63–80.
Lazarus, I., Rush, M., Dibiana, E.T., Monks, C.P., 2017. Gendered penalties of divorce on remarriage in Nigeria: a qualitative study. J. Comparative Family Stud. 48 (3), 351–366.
Lazarus, S., 2019a. Where is the money? The intersectionality of the spirit world and the acquisition of wealth. Religions 10 (3), 146 1–20.
Lazarus, S., 2019b. Just married: The synergy between feminist criminology and the tripartite cybercrime framework. Int. Soc. Sci. J. 1–19. https://doi.org/10.1111/issj.12201.
Lochner, L., 2004. Education, work and crime: a human capital approach. Int. Econ. Rev. 45, 811–843.
Longo, M., 2015. Fiction and Social Reality: Literature and Narrative as Sociological Resources. Ashgate Publishing Limited, Surrey.
Machin, S., Marie, O., Vujić, S., 2011. The crime reducing effect of education. Econ. J. 121 (552), 463–484.
Malinowski, B., [1954]2014. Magic, Science and Religion and Other Essays. New York: Read Books Ltd.
Mauss, M., 1925. The Gift. Routledge, London.
Melvin, A.O., Ayotunde, T., 2010. Spirituality in cybercrime (Yahoo Yahoo) activities among youths in South West Nigeria. In: Youth Culture and Net Culture: Online Social Practices. IGI Global, pp. 357–376.
Messerschmidt, J., 1993. Masculinities and Crime: Critique and Reconceptualization of Theory. Rowman and Littlefield, Lantham.
Morris, C., 2018. 'You can't stand on a corner and talk about it…': medicinal cannabis use, impression management and the analytical status of interviews. Methodol. Innov. 11 (1), 1–12.
Mumporeze, N., Prieler, M., 2017. Gender digital divide in Rwanda: a qualitative analysis of socioeconomic factors. Telematics Inform. 34 (7), 1285–1293.
The Nation, 2017. 'EFCC secure 340 convictions in six months', available at: http://thenationonlineng.net/efcc-secures-340-convictions-six-months/, accessed, 20/12/17.
Newburn, T., 2016. Social disadvantage: crime and punishment. In: Dean, H., Platt, L. (Eds.), Social Advantage and Disadvantage. Oxford University Press, Oxford.
Newburn, Tim, Sparks, Richard, 2004. Policy transfer and lessons drawn. In: Newburn, Tim, Sparks, Richard (Eds.), Criminal Justice and Political Cultures: National and International Dimensions of Crime Control. Routledge, London.
Obuah, E., 2010. Combatting corruption in Nigeria: the Nigerian economic and financial crimes (EFCC). African Stud. Q. 12 (1), 17.
Ojedokun, U.A., Eraye, M.C., 2012. Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. Int. J. Cyber Criminol. 6 (2), 1001–1013.
Owen, T., Noble, W., Speed, F.C., 2017. The challenges posed by scammers to online support groups: the 'deserving' and the 'undeserving' victims of scams. In: New Perspectives on Cybercrime. Palgrave Macmillan, London, pp. 213–240.
Payne, B., 2018. White-collar cybercrime: white-collar crime, cybercrime, or both? Criminol. Criminal Justice Law Soc. 19 (3), 16–32.
Peavy, D., 2016. The Benin Monarchy, Olokun and Iha Ominigbọn. J. Benin Edo Stud. 1 (1), 95–127.
Pierce, Steven, 2016. Moral Economies of Corruption. Duke University Press, Durham, NC, pp. 328.
Polkinghorne, D., 1988. Narrative Knowing and the Human Sciences. State University of New York Press, Albany.
Powell, A., Stratton, G., Cameron, R., 2018. Digital Criminology: Crime and Justice in Digitalsociety. Routledge, New York.
Reiner, R., 2010. The Politics of the Police. Oxford University Press, Oxford.
Reiner, R., 2016. Crime, the Mystery of the Common-Sense Concept. John Wiley & Sons, New York.
Ribbens, J., 1989. Interviewing—an "unnatural situation"? Women's Stud. Int. Forum. 12 (6), 579–592.
Ribbens McCarthy, J., Gillies, V., 2018. Troubling children's families: who is troubled and why? Approaches to inter-cultural dialogue. Sociol. Res. Online 23 (1), 219–244.
Rich, T., 2017. You can trust me: a multimethod analysis of the Nigerian email scam. Security J. 1–18.
Schoepfer, A., Baglivio, M., Schwartz, J., 2017. Juvenile hybrid white-collar delinquency: an empirical examination of various frauds. Criminol. Criminal Justice Law Soc. 18 (1), 18–21.
Selwyn, N., 2008. A safe haven for misbehaving? An investigation of online misbehavior among university students. Social Sci. Comput. Rev. 26 (4), 446–465.
Smith, D.J., 2008. A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria. Princeton University Press.
Smith, D.J., 2017. To be a Man is Not a One-day Job: Masculinity, Money, and Intimacy in Nigeria. University of Chicago Press, Chicago.
Sorell, T., Whitty, M., 2019. Online romance scams and victimhood. Secur. J. 1–20. https://doi.org/10.1057/s41284-019-00166-w.
Swidler, A., 1990. Culture in action: symbols and strategies. Am. Sociol. Rev. 51 (2), 273–286.
Tade, O., 2013. A spiritual dimension to cybercrime in Nigeria: the 'yahoo plus' phenomenon. Human Affairs 23 (4), 689–705.
Tade, O., Aliyu, I., 2011. Social organization of internet fraud among university undergraduates in Nigeria. Int. J. Cyber Criminol. 5 (2), 860–875.
Trend Micro and INTERPOL, 2017. 'Cybercrime in West Africa: Poised for an Underground Market', available at: https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf, accessed 7/7/17.
Umar, I., Samsudin, R.S., Mohamed, M., 2016. Understanding the successes and challenges of anti-corruption agency (ACA) in Nigeria: a case of economic and financial crimes commission (EFCC). Asian J. Multidisciplinary Stud. 4 (5).
UNODC, 2017. 'Supporting the EFCC and Nigerian Judiciary', retrieved: https://www.unodc.org/nigeria/en/s08anticorruption.html, accessed 3/3/18.
Wall, D.S., 2007. Policing cybercrimes: situating the public police in networks of security within cyberspace. Police Practice Res. 8 (2), 183–205.
West, C., Zimmerman, D.H., 1987. Doing gender. In: Fenstermaker, S., West, C. (Eds.), Doing Gender, Doing Difference. Routledge, New York, pp. 3–24.
Whitaker, R., 2013. Proto-spam: Spanish prisoners and confidence games. Retrieved from. The Appendix 1 (4). http://theappendix.net/issues/2013/10/protospam-spanish-prisoners-and-confidence-games.
Yar, M., 2017. Online crime. In: Pontell, Henry (Ed.), Oxford research Encyclopedia of Criminology: Criminology & Criminal Justice. Oxford University Press, Oxford.

Suleman Lazarus is an Austrian independent scholar who is currently a visiting lecturer at the University of Greenwich, United Kingdom. He is a qualitative sociologist and his research interests include the cultural dimensions of digital crimes. While he completed an empirical study on the connections between hip hop artists and cybercriminals in 2018, one of his theoretical works in 2019 nuances "the synergy between feminist criminology and the Tripartite Cybercrime Framework." He is also a published poet and his most recent poem is entitled, "Betrayals in Academia and a Black Demon from Ephesus."

Geoffrey U. Okolorie is a digital forensics expert, a fraud examiner and cybercrime investigator who is currently a postgraduate research student in the UK. He is a member of the Economic and Financial Crimes Commission (EFCC), Nigeria, as well as a member of various local and international professional organizations.